

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-316951

(43)公開日 平成8年(1996)11月29日

(51) Int.Cl. ⁶	識別記号	序内整理番号	F I	技術表示箇所
H 04 L 9/06			H 04 L 9/02	Z
	9/14		H 04 B 14/04	D
H 04 Q 7/38		7259-5 J	G 09 C 1/00	
H 04 B 14/04			H 04 B 7/26	109 R
// G 09 C 1/00			H 04 Q 7/04	D
審査請求 未請求 請求項の数35 O.L (全38頁)				

(21)出願番号 特願平7-123369

(22)出願日 平成7年(1995)5月23日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 小出 歩

神奈川県横浜市戸塚区戸塚町216番地株式

会社日立製作所情報通信事業部内

(72)発明者 黒木 芳徳

神奈川県横浜市戸塚区戸塚町216番地株式

会社日立製作所情報通信事業部内

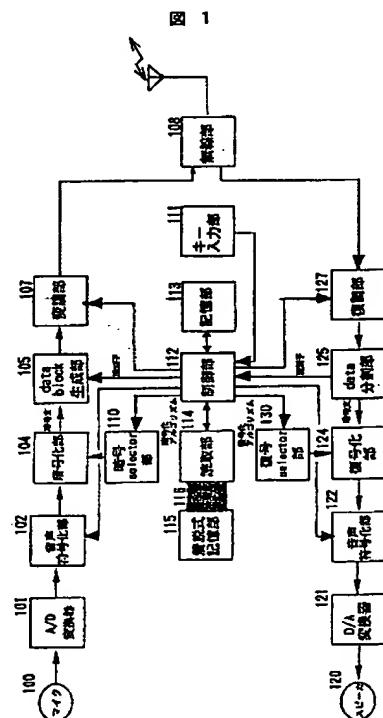
(74)代理人 弁理士 小川 勝男

(54)【発明の名称】 無線通信端末、無線基地局及びこれらを有する通信システム

(57)【要約】

【目的】本発明は、暗号化アルゴリズムを記憶した着脱記憶装置により柔軟、かつ容易に新しい暗号化等へ対応できる無線通信端末及び着脱式記憶装置提供するものである。

【構成】複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶部115を、本体カバーを開けずに装着可能とした装着部116へ装着し、暗号選択部110で暗号化アルゴリズムを選択し、暗号化部104でこの選択された任意の暗号化アルゴリズムに基づいて音声データを暗号化し暗号文を出力する。また、暗号データプロック生成部105で選択された暗号化アルゴリズムに対応する識別子を暗号化テーブルを参照して読みだし前記暗号文に付加して暗号データプロックを出力する。



【特許請求の範囲】

【請求項1】入力された音声をデジタル化し暗号化し通信を行う無線通信端末において、
装着部と、

前記装着部に着脱可能に装着され、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、

前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、

前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が outputする前記音声符号化データを暗号化し暗号文を outputする暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを outputする暗号データブロック生成部と、

前記暗号データブロック生成部が outputする前記暗号データブロックに変調を施し変調データを outputする変調処理部と、

前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。

【請求項2】基地局と多元接続により通信を行う無線通信端末において、

前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、

前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データブロックを取り出し outputする誤り復調処理部と、

前記復調処理部が outputする前記誤り訂正符号化データブロック中の誤りを検出し誤りを訂正し暗号データブロックを outputする誤り訂正符号化部と、

前記誤り訂正符号化部が outputする前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ outputするデータ分割部と、

複数の該復号化アルゴリズムと該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する着脱可能な記憶部と、

前記記憶部を装着する装着部と、

前記記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から outputされる識別子に対応する復号化アルゴリズムを選択する復号選択部と、

前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを outputする復号化部と、

前記復号化に接続され前記音声符号化データを復号しデジタル音声を outputする音声復号化部と、

前記音声復号化部の出力する前記デジタル音声をアナログ化しアナログ音声を outputするアナログ変換部と、前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部と、を有する無線通信端末。

【請求項3】アナログ音声が inputされる音声入力部と、前記音声入力部から inputされる前記アナログ音声をデジタル音声信号に変換し outputするデジタル変換部と、前記デジタル変換部が outputする前記デジタル音声信号を音声符号化データに音声符号化し outputする音声符号化部と、

複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、

前記複数の暗号化アルゴリズムのうちの何れか一つを選択する暗号選択部と、

前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が outputする前記音声符号化データを暗号化し暗号文を outputする暗号化部と、

前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを outputする暗号データブロック生成部と、

前記暗号データブロック生成部が outputする前記暗号データブロックに誤り訂正符号化を施し誤り訂正符号化データブロックを outputする誤り訂正符号化部と、

前記誤り訂正符号化部が outputする前記誤り訂正符号化データブロックに変調を施し変調データを outputする変調処理部と、

前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。

【請求項4】基地局と多元接続により通信を行う無線通信端末において、

前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、

前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データブロックを取り出し outputする誤り復調処理部と、

前記復調処理部が outputする前記誤り訂正符号化データブロック中の誤りを検出し誤りを訂正し暗号データブロックを outputする誤り訂正符号化部と、

前記誤り訂正符号化部が outputする前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ outputするデータ分割部と、

複数の該復号化アルゴリズムと、該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、

前記記憶部に記憶される前記復号化テーブルを参照し前

記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、
 前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、
 前記復号化に接続され前記音声符号化データを復号しデジタル音声を出力する音声復号化部と、
 前記音声復号化部の出力する前記ディジタル音声をアナログ化しアナログ音声を出力するアナログ変換部と、
 前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部と、を有する無線通信端末。
【請求項5】 アナログ音声が入力される音声入力部と、
 前記音声入力部から入力される前記アナログ音声をデジタル音声信号に変換し出力するデジタル変換部と、
 前記ディジタル変換部が出力する前記ディジタル音声信号を音声符号化データに音声符号化し出力する音声符号化部と、
 外部ディジタルデータを入力するための外部インターフェース部と、
 前記音声符号化データと前記外部ディジタルデータとのいずれか一方を選択し出力するデータ選択部と、
 複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
 前記複数の暗号化アルゴリズムのうちの何れか一つを選択する暗号選択部と、
 前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記データ選択部により選択されたデータを暗号化し暗号文を出力する暗号化部と、
 前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データ生成部と、
 前記暗号データブロック生成部が outputする前記暗号データブロックに誤り訂正符号化を施し誤り訂正符号化データブロックを出力する誤り訂正符号化部と、
 前記誤り訂正符号化部が出力する前記誤り訂正符号化データブロックに変調を施し変調データを出力する変調処理部と、
 前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。
【請求項6】 基地局と多元接続により通信を行う無線通信端末において、
 前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、
 前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データブロックを取り出し出力する誤り復調処理部と、

10

20

30

40

50

前記復調処理部が出力する前記誤り訂正符号化データブロック中の誤りを検出し誤りを訂正し暗号データブロックを出力する誤り訂正符号化部と、
 前記誤り訂正符号化部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ出力するデータ分割部と、
 複数の該復号化アルゴリズムと、該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、
 前記記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、
 前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、
 前記復号化部が出力する前記復号データが音声符号化データであるか、あるいはディジタルデータであるかを判定する判定部と、
 前記判定部に接続され前記ディジタルデータを外部へ出力するインターフェースとなる外部インターフェース部と、
 前記判定部に接続され前記音声符号化データを復号しデジタル音声を出力する音声復号化部と、
 前記音声復号化部の出力する前記ディジタル音声をアナログ化しアナログ音声を出力するアナログ変換部と、
 前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部と、を有する無線通信端末。
【請求項7】 アナログ音声が入力される音声入力部と、
 前記音声入力部から入力される前記アナログ音声をデジタル音声信号に変換し出力するデジタル変換部と、
 前記ディジタル変換部が出力する前記ディジタル音声信号を音声符号化データに音声符号化し出力する音声符号化部と、
 外部ディジタルデータを入力するための外部インターフェース部と、
 前記音声符号化データと前記外部ディジタルデータとのいずれか一方を選択し出力するデータ選択部と、
 複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
 前記複数の暗号化アルゴリズムのうちの何れか一つを選択する暗号選択部と、
 前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記データ選択部により選択されたデータを暗号化し暗号文を出力する暗号化部と、
 前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし所定の識別子暗号化アルゴリズムにより暗号化し出力する識別子暗号化部と、前記識別子暗号化部が出力す

る暗号化された識別子を前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、前記暗号データブロック生成部が出力する前記暗号データブロックに誤り訂正符号化を施し誤り訂正符号化データブロックを出力する誤り訂正符号化部と、前記誤り訂正符号化部が出力する前記誤り訂正符号化データブロックに変調を施し変調データを出力する変調処理部と、前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。

【請求項8】基地局と多元接続により通信を行う通信端末において、前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データブロックを取り出し出力する誤り復調処理部と、前記復調処理部が出力する前記誤り訂正符号化データブロック中の誤りを検出し誤りを訂正し暗号データブロックを出力する誤り訂正符号化部と、前記誤り訂正符号化部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する暗号化された識別子を取り出しそれぞれ出力するデータ分割部と、複数の前記復号化アルゴリズムと、該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、前記受信データ分割部から出力される前記暗号化された識別子を復号化し識別子を出力する識別子復号化部と、前記識別子復号化部の出力する前記識別子を前記記憶部に記憶される前記復号化テーブルを参照し対応する復号化アルゴリズムを選択する復号選択部と、前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、前記復号化部が出力する前記復号データが音声符号化データであるか、あるいはディジタルデータであるかを判定する判定部と、前記判定部に接続され前記ディジタルデータを外部へ出力するインターフェースとなる外部インターフェース部と、前記判定部に接続され前記音声符号化データを復号しデジタル音声を出力する音声復号化部と、前記音声復号化部の出力する前記ディジタル音声をアナログ化しアナログ音声を出力するアナログ変換部と、前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部と、を有する無線通信端末。

【請求項9】請求項3乃至8に記載の無線通信端末において、前記記憶部は着脱交換可能なメモリであり、予め任意の

暗号化／復号化アルゴリズムを記憶しておくことを特徴とする無線通信端末。

【請求項10】請求項3乃至8に記載の無線通信端末において、

前記記憶部は、

予め任意の暗号化／復号化アルゴリズムが記憶される着脱交換可能な電子カードと、

前記電子カードに電源を供給し情報を送受する電子カード読み取り部とを有することを特徴とする無線通信端末。

10 【請求項11】暗号化／復号化を施し通信を行う無線通信端末において、

前記暗号化／復号化に用いられる少なくとも一つの暗号と該暗号の識別に用いられる暗号識別子とを記憶する着脱可能な記憶手段と、

該記憶手段を着脱交換可能に装着する装着手段と、

前記装着手段に接続され前記記憶部に記憶された情報を読み出す読み出手段と、

前記読み出手段を制御する制御手段と、を有することを特徴とする無線通信端末。

20 【請求項12】請求項1乃至11に記載の無線通信端末において、

前記記憶部はカード型のメモリであることを特徴とする無線通信端末。

【請求項13】請求項1乃至12に記載の無線通信端末において、

前記暗号化選択部に対し選択すべき暗号化アルゴリズムを指示する制御信号を発する制御手段を有することを特徴とする無線通信端末。

30 【請求項14】請求項13に記載の無線通信端末において、

前記通信端末はキー入力部を有し、

前記キー入力部から入力される入力データに基づいて前記制御部が前記制御信号を発することを特徴とする無線通信端末。

【請求項15】入力された音声をデジタル化し暗号化し通信を行う無線通信端末において、

複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶部を装着すべく成る装着部と、

40 前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、

前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が出力する前記音声符号化データを暗号化し暗号文を出力する暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、

前記暗号データブロック生成部が出力する前記暗号データブロック生成部と、

タブロックに変調を施し変調データを出力する変調処理部と、

前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線通信端末。

【請求項16】移動体通信に用いられる暗号化アルゴリズムを格納する記憶装置において、複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶装置。

【請求項17】請求項16に記載の着脱式記憶装置において、

前記着脱式記憶装置はカード型のメモリであることを特徴とする着脱式記憶装置。

【請求項18】無線通信端末と通信を行なう無線基地局において、

記憶部を装着すべくなる装着部と、

前記装着部に着脱可能に装着され、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、

前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、

前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいてデータを暗号化し暗号文を出力する暗号化部と、

前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、

前記暗号データブロック生成部が outputする前記暗号データブロックに変調を施し変調データを出力する変調処理部と、

前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有することを特徴とする無線基地局。

【請求項19】無線通信端末と通信を行う無線基地局において、

前記無線通信端末が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、

前記無線受信部が取り出す変調信号に復調処理を施し暗号データブロックを出力する復調処理部と、

前記復調処理部が outputする前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ出力するデータ分割部と、

複数の該復号化アルゴリズムと該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶す

る着脱可能な記憶部と、

前記着脱式記憶部を装着する装着部と、

前記着脱式記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、

前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部と、を有する無線基地局。

【請求項20】請求項18、19のいずれかに記載の無線基地局において、

前記記憶部は着脱交換可能なメモリであり、予め任意の暗号化／復号化アルゴリズムを記憶しておくことを特徴とする無線基地局。

【請求項21】請求項18、19のいずれかに記載の無線基地局において、

前記記憶部は、

予め任意の暗号化／復号化アルゴリズムが記憶されるメモリを内蔵した着脱交換可能な電子カードと、

前記電子カードに電源を供給し情報を送受する電子カード読取り部とを有することを特徴とする無線基地局。

【請求項22】暗号化／復号化を施し通信を行う無線基地局において、

前記暗号化／復号化に用いられる少なくとも一つの暗号と該暗号の識別に用いられる暗号識別子とを記憶する着脱可能な記憶手段と、

該記憶手段を着脱交換可能に装着する装着手段と、

前記装着手段に接続され前記記憶部に記憶された情報を読み出す読出手段と、

前記読出手段を制御する制御手段と、を有することを特徴とする無線基地局。

【請求項23】請求項18乃至21に記載の無線基地局において、

前記暗号化選択部に対し選択すべき暗号化アルゴリズムを指示する制御信号を発する制御手段を有することを特徴とする無線基地局。

【請求項24】複数の無線通信端末と暗号化を施し通信を行なう無線基地局において、

複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶部を装着すべく成る装着部と、

前記複数の暗号化アルゴリズムのうち前記無線通信端末が備えている暗号化アルゴリズムと共通のもののうちの何れか一つを選択する暗号選択部と、

前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が outputする前記音声符号化データを暗号化し暗号文を出力する暗号化部と、

前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する

暗号データブロック生成部と、
前記暗号データブロック生成部が outputする前記暗号データブロックに変調を施し変調データを outputする変調処理部と、
前記変調処理部の outputする前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有する無線基地局。

【請求項25】無線通信端末と暗号化を施し通信を行なう無線基地局を管理する管理局において、
複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
前記記憶部に記憶された暗号化テーブルを前記無線基地局に送信する送信部と、
前記記憶部及び送信部を制御する制御部と、を有することを特徴とする管理局。

【請求項26】無線通信端末との暗号化通信に用いられる暗号化テーブルを所有する無線基地局を管理する管理局において、
複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、

前記記憶部に記憶された暗号化テーブルを前記無線基地局への送信と、及び、該送信された暗号化テーブルに基づいて前記無線基地局の所有する暗号化テーブルを更新するよう命令する命令信号の送信とを行なう送信部と、前記記憶部及び送信部を制御する制御部と、を有することを特徴とする管理局。

【請求項27】管理局によって管理され、無線通信端末と暗号化を施し通信を行なう無線基地局において、前記管理局から送信される命令信号に基づいて、前記管理局から送信されてきた暗号化テーブルを記憶する記憶部を有することを特徴とする無線基地局。

【請求項28】管理局に管理され、無線通信端末と通信を行う無線基地局において、
前記無線通信端末が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、
前記無線受信部が取り出す変調信号に復調処理を施し暗号データブロックを outputする復調処理部と、
前記復調処理部が outputする前記暗号データブロックから暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子とを取り出しそれぞれ outputするデータ分割部と、

複数の該復号化アルゴリズムと該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、
前記着脱式記憶部に記憶される前記復号化テーブルを參照し前記受信データ分割部から outputされる識別子に対応

する復号化アルゴリズムを選択する復号選択部と、
前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを outputする復号化部と、を有し、
前記管理局が送信する暗号化テーブルに基づいて前記記憶部に記憶される暗号化テーブルを更新することを特徴とする無線基地局。

【請求項29】無線通信端末と通信を行なう無線基地局において、

10 複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、
前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、

前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいてデータを暗号化し暗号文を outputする暗号化部と、
前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを outputする暗号データブロック生成部と、

前記暗号データブロック生成部が outputする前記暗号データブロックに変調を施し変調データを outputする変調処理部と、
前記変調処理部の outputする前記変調データを所定の無線チャネルに割り当て送信する無線送信部と、を有し、
前記管理局が送信する暗号化テーブルに基づいて、前記記憶部に記憶された暗号化テーブルを更新することを特徴とする無線基地局。

20 【請求項30】第1の無線通信端末と第2の無線通信端末とが無線基地局を介して通信を行なう通信システムにおいて、
前記第1の無線通信端末は、
前記無線基地局との暗号化通信に用いられる第1の暗号化／復号化アルゴリズムを有し、
前記第2の無線通信端末は、
前記無線基地局との暗号化通信に用いられる第1の暗号化／復号化アルゴリズムとは異なる第2の暗号化／復号化アルゴリズムを少なくとも有し、
前記基地局は、前記第1の暗号化／復号化アルゴリズム及び第2の暗号化／復号化アルゴリズムを有することを特徴とする通信システム。

40 【請求項31】第1の無線通信端末と、該第1の無線通信端末と無線通信を行なう第1の無線基地局と、該第1の無線基地局と通信を行なう第2の無線基地局と、該第2の無線基地局と無線通信を行なう第2の無線通信端末とを有する通信システムにおいて、
前記第1の無線通信端末は、
前記第1の無線基地局との暗号化通信に用いられる第1

50

の暗号化／復号化アルゴリズムを有し、
前記第2の無線通信端末は、
前記第2の基地局との暗号化通信に用いられる第1の暗号化／復号化アルゴリズムとは異なる第2の暗号化／復号化アルゴリズムを少なくとも有し、
前記第1の無線基地局は、
少なくとも前記第1の暗号化／復号化アルゴリズムを有し、
前記第2の無線基地局は、
少なくとも前記第2の暗号化／復号化アルゴリズムを有することを特徴とする通信システム。

【請求項32】第1の無線通信端末と第2の無線通信端末とが無線基地局を介して通信を行なう通信システムにおいて、

前記第1の無線通信端末は、
前記無線基地局を介して前記第2の無線通信端末との暗号化通信に用いられる暗号化／復号化アルゴリズムを有し、
前記第2の無線通信端末は、
前記第1の無線通信端末との暗号化通信に用いられる前記暗号化／復号化アルゴリズムと、
前記暗号化／復号化アルゴリズムとは異なる暗号化アルゴリズムを少なくとも一つ有することを特徴とする通信システム。

【請求項33】第1の無線通信端末と、該第1の無線通信端末と無線通信を行なう第1の無線基地局と、該第1の無線基地局と通信を行なう第2の無線基地局と、該第2の無線基地局と無線通信を行なう第2の無線通信端末とを有する通信システムにおいて、

前記第1の無線通信端末は、
前記第1の無線基地局及び前記第2の無線基地局とを介して前記第2の無線通信端末との暗号化通信に用いられる暗号化／復号化アルゴリズムを有し、
前記第2の無線通信端末は、
前記第2の無線基地局及び前記第1の無線基地局とを介して前記第1の無線通信端末との暗号化通信に用いられる前記暗号化／復号化アルゴリズムと、
前記暗号化／復号化アルゴリズムとは異なる他の暗号化／復号化アルゴリズムを少なくとも一つ有することを特徴とする通信システム。

【請求項34】無線通信に用いられる暗号化方法において、
音声を入力し、
前記入力された音声を音声符号化して情報圧縮し、
前記情報圧縮された音声に対し暗号化を施す複数の暗号化アルゴリズムから一つを選択し、
前記選択された暗号化アルゴリズムに基づいて情報圧縮された音声を暗号化し、
前記暗号化アルゴリズムに対応する識別子を識別子暗号化し、

前記暗号化された音声と前記識別子暗号化された識別子とを一つデータへとデータブロック化し、
前記データブロック化されたデータを送信することを特徴とする暗号化方法。

【請求項35】無線通信に用いられる復号化方法において、

受信データから暗号文と識別子暗号文を抽出分離し、
前記識別子暗号文から識別子を復号化し、
復号された識別子に基づいて前記暗号文を復号化する復号化アルゴリズムを選択し、
選択された復号化アルゴリズムで暗号文を復号化し音声圧縮情報を出力し、
前記音声圧縮情報を情報伸長し、音声を出力することを特徴とする復号化方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、通信回路や各種通信回線等を経由して情報の送受信を行う情報通信機器に応用される、暗号化／復号化装置を有する無線通信端末、無線基地局及びこれらを有する通信システムに関する。

【0002】

【従来の技術】暗号化を施し通信を行う技術として、特表平6-506813に開示されているような暗号化通信方法がある。この暗号化通信方法では、無線機に複数の暗号化キーとそれらに対応するキー識別子とを備え、送信側無線機でキー識別子を選択し、選択されたキー識別子に対応した暗号化キーで平文を暗号化して暗号文を生成し、暗号化に用いたキー識別子と共に暗号文を相手無線機に送信し、相手無線機では、送られてきたキー識別子に基づいて暗号文を解読することが提案されている。

【0003】一方で、携帯無線電話システムであるピー・エイチ・エス（以下PHSと称す）では、スクランブル／デスクランブル処理あるいは簡易秘話処理をもつて通信端末と基地局の間で暗号化を行っている。

【0004】

【発明が解決しようとする課題】上記のようにPHSでは、暗号化／復号化アルゴリズムとしてスクランブルあるいは簡易秘話をもつて暗号化処理を行い、任意の端末間あるいは、端末と基地局間で情報の伝送を行っている。

【0005】しかし、上述したスクランブルと簡易秘話は簡略的なものであり、盗聴者によって容易に解読されるものである。今後はセキュリティの確保が一層求められるため、暗号化アルゴリズムを公開しても解読が困難な、より強力な暗号化を行わなければならないという第一の課題がある。

【0006】現状では、スクランブルと簡易秘話以外の暗号化はオプションであり、今後各メーカーごとに様々な暗号化アルゴリズムを備えた無線通信端末が製品化さ

れよう。このような状況下では、あるメーカーのP H S 端末（既存端末）で暗号化された暗号文は、通信端末を製造するメーカーの基地局（基地局側）のみでしか復号化できない状態になりうる。すなわち、同じメーカー製の同じ暗号化アルゴリズムを備えた特定の端末と基地局間、又は特定の端末間だけでしか情報の送受信を行うことができなくなる。また、今後新しい暗号化アルゴリズムが開発され、上記と同じようにその新しい暗号化アルゴリズムを備えた特定の端末と基地局間、又は特定の端末間だけでしか情報の送受信を行うことができなくなるという第2の課題がある。情報通信の発展に伴い、このような課題が障害となることは確実である。

【0007】本発明の目的は、移動体電話通信において強力な暗号化を有する無線通信端末を提供することにある。

【0008】さらに本発明の他の目的は、複数の異なった暗号化／復号化アルゴリズムを備えた無線通信端末との通信を可能とし、さらに、新しい暗号化／復号化アルゴリズムが提供されたときにも、新しいアルゴリズムを記憶した着脱交換式メモリにより柔軟、かつ、容易に対処できることにある。

【0009】

【課題を解決するための手段】本発明の無線通信端末には、装着部と、前記装着部に着脱可能に装着され、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が出力する前記音声符号化データを暗号化し暗号文を出力する暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データロックを出力する暗号データロック生成部と、前記暗号データロック生成部が出力する前記暗号データロックに誤り訂正符号化を施し誤り訂正符号化データロックを出力する誤り訂正符号化部と、前記誤り訂正符号化部が出力する前記誤り訂正符号化データロックに変調を施し変調データを出力する変調処理部と、前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部とを設けた。

【0010】本発明の無線通信端末は、アナログ音声を入力する音声入力部と、前記音声入力部から入力される前記アナログ音声をデジタル音声信号に変換し出力するデジタル変換部と、前記デジタル変換部が出力する前記デジタル音声信号を音声符号化データに音声符号化し出力する音声符号化部と、外部デジタルデータを入力するための外部インターフェース部と、前記音

声符号化データと前記外部デジタルデータとのいずれか一方を選択し出力するデータ選択部と、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記複数の暗号化アルゴリズムのうちの何れか一つを選択する暗号選択部と、前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記データ選択部により選択されるデータを暗号化し暗号文を出力する暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし所定の識別子暗号化アルゴリズムにより暗号化し出力する識別子暗号化部と、前記識別子暗号化部が出力する暗号化された識別子を前記暗号文に付加し暗号データロックを出力する暗号データロック生成部と、前記暗号データロック生成部が出力する前記暗号データロックに誤り訂正符号化を施し誤り訂正符号化データロックを出力する誤り訂正符号化部と、前記誤り訂正符号化部が出力する前記誤り訂正符号化データロックに変調を施し変調データを出力する変調処理部と、前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部とを設けた。

【0011】また、本発明の無線通信端末は、基地局と多元接続により通信を行う通信端末において、前記基地局が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、前記無線受信部が取り出す変調信号に復調処理を施し誤り訂正符号化データロックを取り出し出力する誤り復調処理部と、前記復調処理部が出力する前記誤り訂正符号化データロック中の誤りを検出し誤りを訂正し暗号データロックを出力する誤り訂正符号化部と、前記誤り訂正符号化部が出力する前記暗号データロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する暗号化された識別子を取り出しそれぞれ出力するデータ分割部と、複数の前記復号化アルゴリズムと、該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、前記受信データ分割部から出力される前記暗号化された識別子を復号化し識別子を出力する識別子復号化部と、前記識別子復号化部の出力する前記識別子を前記記憶部に記憶される前記復号化テーブルを参照し対応する復号化アルゴリズムを選択する復号選択部と、前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力するする復号化部と、前記復号化部が出力する前記復号データが音声符号化データであるか、あるいはディジタルデータであるかを判定する判定部と、前記判定部に接続され前記ディジタルデータを外部へ出力するインタフェースとなる外部インターフェース部と、前記判定部に接続され前記音声符号化データを復号しディジタル音声を出力す

30
20
30
40
50

る音声復号化部と、前記音声復号化部の出力する前記デジタル音声をアナログ化しアナログ音声を出力するアナログ変換部と、前記アナログ変換部の出力するアナログ音声を外部に出力する音声出力部とを設けた。

【0012】また、本発明の無線通信端末は、前記記憶部は着脱交換可能なメモリであり、予め任意の暗号化／復号化アルゴリズムを記憶しておくことを特徴とする。

【0013】また、本発明の無線通信端末は、前記暗号化／復号化に用いられる少なくとも一つの暗号と該暗号の識別に用いられる暗号識別子とを記憶する着脱可能な記憶手段と、該記憶手段を着脱可能に装着する装着手段と、前記装着手段に接続され前記記憶部に記憶された情報を読み出す読出手段と、前記読出手段を制御する制御手段とを設けた。

【0014】また、本発明の着脱式記憶装置は、メモリをカード形状の筐体に納めた。

【0015】また、本発明の無線基地局は、記憶部を装着するべくなる装着部と、前記装着部に着脱可能に装着され、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と、該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記複数の暗号化アルゴリズムのうち何れか一つを選択する暗号選択部と、前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいてデータを暗号化し暗号文を出力する暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号データブロックを出力する暗号データブロック生成部と、前記暗号データブロック生成部が生成する前記暗号データブロックに変調を施し変調データを出力する変調処理部と、前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部とを設けた。

【0016】また、本発明の無線基地局は、前記無線通信端末が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、前記無線受信部が取り出す変調信号に復調処理を施し暗号データブロックを出力する復調処理部と、前記復調処理部が出力する前記暗号データブロックより暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子を取り出しそれぞれ出力するデータ分割部と、複数の該復号化アルゴリズムと該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する着脱可能な記憶部と、前記着脱式記憶部を装着する装着部と、前記着脱式記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と、前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部とを設けた。

【0017】また、本発明の無線基地局は、暗号化／復

号化に用いられる少なくとも一つの暗号と該暗号の識別に用いられる暗号識別子とを記憶する着脱可能な記憶手段と、該記憶手段を着脱交換可能に装着する装着手段と、前記装着手段に接続され前記記憶部に記憶された情報を読み出す読出手段と、前記読出手段を制御する制御手段とを設けた。

【0018】また、本発明の無線基地局は、複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する着脱式記憶部を装着すべく成る装着部と、前記複数の暗号化アルゴリズムのうち前記無線通信端末が備えている暗号化アルゴリズムと共通のもののうちの何れか一つを選択する暗号選択部と、前記暗号選択部によって選択される任意の暗号化アルゴリズムに基づいて前記音声符号化部が输出する前記音声符号化データを暗号化し暗号文を出力する暗号化部と、前記暗号化部で用いられる前記任意の暗号化アルゴリズムに対応する識別子を前記暗号化テーブルを参照し読みだし前記暗号文に付加し暗号

20 データブロックを出力する暗号データブロック生成部と、前記暗号データブロック生成部が出力する前記暗号データブロックに変調を施し変調データを出力する変調処理部と、前記変調処理部の出力する前記変調データを所定の無線チャネルに割り当て送信する無線送信部とを設けた。

【0019】また、本発明の管理局は複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記記憶部に記憶された暗号化テーブルを前記無線基地局に送信する送信部と、前記記憶部及び送信部を制御する制御部とを設けた。

【0020】また、本発明の管理局は、複数の暗号化アルゴリズムと該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルとを記憶する記憶部と、前記記憶部に記憶される暗号化テーブルを前記無線基地局への送信と、及び、該送信された暗号化テーブルに基づいて前記無線基地局の所有する暗号化テーブルを更新するよう命令する命令信号の送信とを行なう送信部と、前記記憶部及び送信部を制御する制御部とを設けた。

【0021】また、本発明の無線基地局は、無線通信端末が無線チャネルを介して送信する信号を受信し変調信号を取り出す無線受信部と、前記無線受信部が取り出す変調信号に復調処理を施し暗号データブロックを出力する復調処理部と、前記復調処理部が出力する前記暗号データブロックから暗号文と、該暗号文を復号化する復号化アルゴリズムを指定する識別子を取り出しそれぞれ出力するデータ分割部と、複数の該復号化アルゴリズム

と該復号化アルゴリズムと該識別子との対応関係を表す復号化テーブルとを記憶する記憶部と、前記着脱式記憶部に記憶される前記復号化テーブルを参照し前記受信データ分割部から出力される識別子に対応する復号化アルゴリズムを選択する復号選択部と前記復号選択部によって選択される復号化アルゴリズムに基づいて前記暗号文を復号し復号データを出力する復号化部とを設け、前記管理局が送信する暗号化テーブルに基づいて前記記憶部に記憶される暗号化テーブルを更新する。

【0022】また、本発明の無線通信システムは、第1の無線通信端末は、前記無線基地局との暗号化通信に用いられる第1の暗号化／復号化アルゴリズムを有し、第2の無線通信端末は、無線基地局との暗号化通信に用いられる第1の暗号化／復号化アルゴリズムとは異なる第2の暗号化／復号化アルゴリズムを少なくとも一つ有し、無線基地局は、前記第1の暗号化／復号化アルゴリズム及び第2の暗号化／復号化アルゴリズムを有する。

【0023】また、本発明の通信システムは第1の無線通信端末は、前記第1の無線基地局との暗号化通信に用いられる第1の暗号化／復号化アルゴリズムを有し、第2の無線通信端末は、前記第2の基地局との暗号化通信に用いられる第1の暗号化／復号化アルゴリズムとは異なる第2の暗号化／復号化アルゴリズムを少なくとも有し、第1の無線基地局は、少なくとも前記第1の暗号化／復号化アルゴリズムを有し、第2の無線基地局は、少なくとも前記第2の暗号化／復号化アルゴリズムを有する。

【0024】また、本発明の通信システムは、第1の無線通信端末は、前記無線基地局を介して第2の無線通信端末との暗号化通信に用いられる暗号化／復号化アルゴリズムを有し、前記第2の無線通信端末は、前記第1の無線通信端末との暗号化通信に用いられる前記暗号化／復号化アルゴリズムと、前記暗号化／復号化アルゴリズムとは異なる暗号化アルゴリズムを少なくとも一つ有する。

【0025】また、本発明の通信システムは、第1の無線通信端末は、前記第1の無線基地局及び前記第2の無線基地局とを介して前記第2の無線通信端末との暗号化通信に用いられる暗号化／復号化アルゴリズムを有し、第2の無線通信端末は、第2の無線基地局及び第1の無線基地局とを介して前記第1の無線通信端末との暗号化通信に用いられる前記暗号化／復号化アルゴリズムと、前記暗号化／復号化アルゴリズムとは異なる他の暗号化／復号化アルゴリズムを少なくとも一つ有する。

【0026】

【作用】本発明の無線通信端末は盗聴防止のため、端末ユーザの暗号化アルゴリズム変更要求時に、キー入力等の手段によって任意に又は呼接続時毎に、位置登録時毎に、通話中チャネル切り替え時毎に、認証時毎に、予め定められた時間毎に、全くランダムに、予め定められた

エリア毎に端末が暗号化アルゴリズムを切り替えるため、暗号の解読がされにくくなる。また、複数の暗号化アルゴリズムと対応する暗号化アルゴリズム識別子をメモリ等の記憶手段に格納していて、CPU等の手段が暗号化アルゴリズム識別子のビット数に対応する乱数を任意の乱数発生器で出し、出力された乱数を用い暗号化テーブルから暗号化アルゴリズムを選択し、暗号化アルゴリズムを切り替えてよい。その後、前記暗号化アルゴリズムでメッセージの暗号化を行い暗号文を出力し、同時に任意の暗号化アルゴリズムで暗号化アルゴリズムを識別するための識別子を暗号化する。前記暗号文は識別子暗号文と共に受信側へ伝送される。

【0027】本発明の無線通信端末は、送信側から伝送されてきた暗号文と識別子暗号文を受け取り、識別子暗号文を任意の復号化アルゴリズムで復号化する。復号化された識別子からどの暗号化アルゴリズムを使用しているかを判断し、対応する復号化アルゴリズムを選択する。前記復号化装置は、前記暗号化装置に対応して、複数の復号化アルゴリズムをROM等の手段に格納していて、選択された復号化アルゴリズムを切り替え、前記復号化アルゴリズムを用いて暗号文をメッセージに復号化する。

【0028】本発明の無線通信端末は、暗号化アルゴリズム、識別子及び暗号化テーブルを記憶する記憶部が着脱可能であるため、改めて新しい暗号化アルゴリズムが提供された場合に、新しい暗号化アルゴリズムを含めて記憶した記憶部を脱着交換すれば容易に他の暗号化アルゴリズムをサポートすることができる。

【0029】上記のように無線通信端末を構成することによって、同じ暗号化アルゴリズムを備えた特定の端末基地局間だけでしか情報の伝送を行うことができないという課題を克服することができる。

【0030】本発明の無線基地局は、着脱交換式の記憶部を設けることにより容易に新しい暗号化アルゴリズムを網羅することが出来る。

【0031】また本発明の管理局は、全ての暗号化テーブルを備え、この最新の暗号化テーブルを管理下にある複数の無線基地局に対して送信すると共に、無線基地局には、無線基地局の有する記憶部内の暗号化テーブルを更新するよう命令する。

【0032】この管理局によって、無線基地局は容易に新しい暗号化アルゴリズムにも対処できる。またこの構成であれば、着脱交換式メモリは必要ないためコスト的に有利である。

【0033】また、本発明の通信システムでは、通信を行なう二つの無線通信端末のうち、片方が相手方と同じ暗号化アルゴリズムを含め複数備えているので、新しい暗号化アルゴリズムを備えていない無線通信端末とも通信できる。

【0034】また、本発明の通信システムは無線通信端

未間を仲介する無線基地局が、全ての暗号化アルゴリズムを備えることで、暗号変換部としての役割を果たすため、通信しようとする無線通信端末間で共通する暗号化アルゴリズムが存在しない場合であっても暗号化通信を可能としている。

【0035】

【実施例】本発明の実施例について PHS を例に図を参考して説明する。

【0036】本発明の暗号化・復号化装置を備えた PHS 端末機能図を送信部と受信部に分けて説明する。図1には本発明を実施する場合の一例である無線通信端末を示す。また図2, 3は無線通信端末の送信部のみを示した図である。図1、2、3に示すように、無線通信端末である PHS 端末の送信部は、音声を入力するマイクと、音声をデジタル化する A/D 変換器と、ADPCM や VSEL P または P R E - L T P などの一般的な音声圧縮を行なう音声符号化部と、マイク入力あるいは外部インターフェースのいずれかを選択する data selector 部と、暗号化を施す暗号化部と、暗号文に識別子を付加する data block 生成部と、誤り訂正符号化を施す誤り検出・訂正符号化部と、情報に対して各種変調方式により多重変調等を行なう変調部及び無線部と、外部からのデータ入力部と成る RS 232 C などの外部インターフェース部と、暗号化に用いられる暗号化アルゴリズムを選択する暗号 selector 部と、ユーザの希望によってキーを押すことで他の暗号化アルゴリズムに切り替えるためのキー入力部と、及び全体を司る制御部と、暗号化アルゴリズムやこの暗号化アルゴリズムの一つ一つに対応する暗号化識別子、及び暗号化アルゴリズム、識別子および暗号化アルゴリズムと識別子との関係を表わす、例えば図4に示したような暗号化テーブルを記憶する記憶部を有して構成される。ここで、制御部は一つであっても複数個備え各処理及び制御を分担してもよい。また、暗号化アルゴリズムと識別子は必ずしも一対一でなくてもよい。というのは、複数の暗号化アルゴリズムを組み合わせて一つの暗号化を施す場合など、複数ある暗号化アルゴリズムの実行順序の関係を識別子をもちいて記述し、テーブルかして記憶すれば、既存の暗号化アルゴリズムを自由に、かつ簡単に組み合わせるだけにより強固な暗号化アルゴリズムを提供できるのである。

【0037】また記憶部は、一つであっても複数であってもよい。ところで、新たな暗号化アルゴリズムが提案されたときに、すばやく対処できるようにするために、記憶部を着脱式にしておき、ユーザが新しい暗号化アルゴリズムが記憶されたメモリカードを自由に購入し、交換してもよい。また、着脱式でなくとも、書替え可能なメモリであってもよい。この場合、ユーザは端末のサービスセンタで書き替えてよいし、電話回線を通じて通信によりダウンロードしてもよい。ダウンロードの場

合、ユーザはキー操作によって制御部に暗号化アルゴリズムをダウンロードする旨を指定し、制御部は電話回線より送られてきた暗号化アルゴリズムと識別子などを記憶部のテーブルに追加書き込みする。

【0038】次に、これらの構成による端末の具体的な信号処理手順を図5に示すフローチャートを参照して説明する。

【0039】まず、ステップ800において、伝送したい音声データをマイク等の手段で又、FAX、パソコン

- 10 等の 32 k b p s データをインターフェースコネクタ等の外部入力端子から入力する。次に、ステップ801において、data selector 部で音声データが PHS 端末に入力されるか判定を行う。音声データが入力されるならばステップ802以降の処理を行い、FAX、パソコン等の 32 k b p s データが入力されるならばステップ804以降の処理を行う。次に、ステップ802において、ディジタル処理を行うために、入力された 300~3400 Hz のアナログ音声信号を A/D 変換器でディジタル信号に変換する。次に、ステップ803において、音声符号化部で音声符号化処理を行い、64 k b p s の PCM データを 32 k b p s の音声符号化ビットに変換する。次に、ステップ804において、ユーザが任意にキーパッド等の手段で暗号化アルゴリズム識別子を入力する。次に、ステップ805において、制御部ではキー入力された暗号化アルゴリズム識別子をスキャンして読みとる。記憶部は、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する暗号化アルゴリズム識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルを備えていて、ステップ806において、暗号 selector 部は制御部で読みとった暗号化アルゴリズム識別子に基づき対応する暗号化アルゴリズムを選定する。次に、ステップ807において、暗号化部で前記音声符号化ビットや FAX、パソコン等の各種データに対して、任意のビット長だけ格納し、そのビット長を 1 ブロックとして暗号 selector 部で選定された暗号化アルゴリズムで暗号化処理を行う。次に、ステップ808において、data block 生成部で、暗号化アルゴリズム識別子と暗号化されたビットのあるブロック (PHS の場合はデータ 160 ビット) 每に格納し、そのブロックごとに誤り検出・訂正符号化部で巡回符号 (CRC) による符号化を行い、データ 160 ビットに符号化されたビットを付け加えるチャネルコーデック処理を行う。次に、ステップ809において、変調部でチャネルコーデック処理によって出力された送信データのデジタル変調 (PHS の場合は $\pi/4$ シフト QPSK) を行う。次に、ステップ810において、無声部で無線チャネルの設定を行い、音声や各種データを無線回線を使って伝送することができる。以上の処理によって、音声や各種データを無線回線を使って送信すること
- 20
- 30
- 40
- 50

ができる。

【0040】次に受信時の処理について説明する。図1、図6及び図7にはPHS端末の受信部を示している。本発明の無線通信端末の実施例では、音声を出力するスピーカと、デジタル信号をアナログ信号にするD/A変換器と、音声圧縮された信号を復号する音声復号化部と、送られてきた暗号文を復号する復号化部と、送られてきた信号から識別子と暗号文とを分離し出力するdata分割部と、誤り検出や誤り訂正を施す誤り検出・訂正部と、送られてきた信号を復調する復調部及び無線部と、RS232C等のインターフェースや文字表示装置である外部インターフェースと、識別子に基づいて暗号文を復号するための復号化アルゴリズムを選択する復号selector部と、全体を統括する制御部と、復号化アルゴリズムや復号化テーブルを記憶する記憶部を有している。

【0041】受信部の処理手順を図8に示し、該フローチャートを参照して処理手順について説明する。受信部では、まずステップ900において無線部で無線チャネルから伝送されてきた信号を受け取る。次に、ステップ901において、復調部で信号の復調処理を行う。次に、ステップ902において、誤り検出・訂正部で送信部と同じように復調処理を行ったビットに対して、あるブロック（PHSの場合はデータ160ビット）毎に、巡回符号（CRC）による符号化を行い、送信部から伝送されてきた巡回符号（CRC）による符号化ビットと比較し、伝送路での誤り検出を行う。次に、ステップ903において、伝送路での誤りが検出されたかどうかの判定を行う。誤りが検出されればステップ904の処理を行い、誤りが検出されなければステップ905の処理を行う。次に、ステップ904において、誤り除去又は低減処理を行う。次に、ステップ905において、data分割部で暗号文と暗号化アルゴリズム識別子を分割する。記憶部は、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する暗号化アルゴリズム識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルを備えていて、ステップ906において、復号selector部は、受信した暗号化アルゴリズム識別子に基づき対応する暗号化アルゴリズムを選定する。次に、ステップ907において、復号化部で情報ビット（PHSの場合は160ビット）に対して、任意のビット長だけ格納し、そのビット長を1ブロックとして復号selector部で選定された復号化アルゴリズムで復号化処理を行う。次に、ステップ908において、data判定部で音声データであるか判定を行う。音声データであればステップ909へ、FAX、パソコン等の32kbpsデータであればステップ910の処理を行う。次に、ステップ911において、音声復号化部で音声復号化処理を行い、音声符号化ビットをデジタル信号に変換する。次に、

10

20

30

40

50

ステップ912において、アナログ信号を得るために（音声を出力するため）、D/A変換器でデジタル信号を300～3400Hzのアナログ音声に変換する。次に、ステップ913において、スピーカ等の手段を通して、音声を出力する。また、ステップ914において、FAX、パソコン等の32kbpsデータをインターフェースコネクタ等の外部入力端子から出力する。以上の処理によって、無線回線から音声や各種データを受信することができる。

【0042】次に、本発明の暗号化・復号化装置を備えた基地局の機能図を送信機能と受信機能について説明する。図9、10にはとりわけ送信部を、図11、12には受信部を示している。基地局の送信機能としては、DSU（デジタル・サービス・ユニット）と、SINFと、エコーリンセラと、音声符号化部と、暗号化部と、data block生成部と、誤り検出・訂正符号化部と、変調部と、無線部と、暗号selector部と、制御部と、記憶部を有して構成される。送信機能としては、まず、PBXから送られてきた2B+D

（B：64kbps, D：16kbps）の信号がDSUを介して基地局に入る。次に、SINF（S-Interface）で2B+Dの信号をBチャネル（情報信号）2つとDチャネル（制御信号）に分割する。次に、エコーリンセラで、回線系エコー（2線→4線変換のハイブリッドでの不整合によるエコー）の消去を行う。次に、音声符号化部で音声符号化処理を行い、64kbpsのデジタル信号を32kbpsのデータに変換する。次に、暗号化アルゴリズム識別子のビット数に対応する乱数を任意の乱数発生器で出力する。記憶部は、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する暗号化アルゴリズム識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルを備えていて、暗号selector部は、乱数発生器で出力された暗号化アルゴリズム識別子に基づき対応する暗号化アルゴリズムを選定する。

次に、暗号化部で前記32kbpsのデータに対して、任意のビット長だけ格納し、そのビット長を1ブロックとして暗号selector部で選定された暗号化アルゴリズムで暗号化処理を行う。次に、data block生成部で暗号化アルゴリズム識別子と暗号化されたビットをあるブロック（PHSの場合はデータ160ビット）毎に格納し、そのブロックごとに誤り検出・訂正符号化部で巡回符号（CRC）による符号化を行い、データ160ビットに符号化されたビットを付け加えるチャネルコーデック処理を行う。次に、変調部でチャネルコーデック処理によって出力された送信データのデジタル変調（PHSの場合はπ/4シフトQPSK）を行う。次に、無線部で無線チャネルの設定を行い、音声や各種データを無線回線を使って伝送することができる。

以上の処理によって、音声や各種データを無線回線を使

って送信することができる。

【0043】受信機能としては、D S Uと、S I N Fと、エコーキャンセラと、音声復号化部と、復号化部と、d a t a 分割部と、誤り検出・訂正部と、復調部と、無線部と、復号s e l e c t o r 部と、制御部と、記憶部を有して構成される。受信時の動作を以下に説明する。受信部では、無線部で無線チャネルから伝送してきた信号を受け取る。次に、復調部で信号の復調処理を行う。次に、誤り検出・訂正部で送信部と同じように復調処理を行ったビットに対して、あるブロック（P H Sの場合データ160ビット）毎に、巡回符号（C R C）による符号化を行い、送信部から伝送されてきた巡回符号（C R C）による符号化ビットと比較し、伝送路での誤り検出を行う。次に、伝送路での誤りが検出されたかどうかの判定を行う。誤りが検出されれば、誤り除去又は低減処理を行う。次に、d a t a 分割部で暗号文と暗号化アルゴリズム識別子を分割する。記憶部は、複数の暗号化アルゴリズムと、該複数の暗号化アルゴリズムの一つ一つにそれぞれ対応する暗号化アルゴリズム識別子と該識別子と該暗号化アルゴリズムとの対応関係を表す暗号化テーブルを備えていて、復号s e l e c t o r 部は、受信した暗号化アルゴリズム識別子に基づき対応する暗号化アルゴリズムを選定する。次に、復号化部で情報ビット（P H Sの場合160ビット）に対して、任意のビット長だけ格納し、そのビット長を1ブロックとして復号s e l e c t o r 部で選定された復号化アルゴリズムで復号化処理を行う。次に、音声復号化部で音声復号化処理を行い、音声符号化ビットをデジタル信号に変換する。次に、エコーキャンセラで、音響系エコー（スピーカーマイク間のエコー）の消去を行う。次に、S I N Fで、Bチャネル（情報信号）2つとDチャネル（制御信号）をまとめて2B+Dの信号を生成する。2B+Dの信号はD S Uを介してP B Xへ伝送される。以上の処理によって、無線回線から音声や各種データを受信し、P B Xへデータ伝送をすることができる。

【0044】GSM、F P L M T Sについてもこの構成で十分である。

【0045】図13は、本発明にかかるP H Sの他の実施例を示している。

【0046】P H Sは、事業所用と屋外用（公衆用）と家庭用に分かれている。事業所用P H Sは、ディジタルコードレス端末300と、事業所内基地局301と、事業所用P B X302を有して構成される。屋外用（公衆用）P H Sは、P H S端末303～304と、屋外基地局305と、モジュールアダプタ306を有して構成される。

【0047】家庭用P H Sは、P H S端末307と、家庭内基地局308を有して構成される。それぞれのシステムは、交換機を介して一般電話機310や他の通信機器と接続される。本発明の暗号化／復号化部は、図に示

すようにそれぞれのシステムの端末、基地局内、又はP B X内に含まれている。

【0048】次に、P H S端末機能図を図14を参照して説明する。

【0049】P H S端末は、全体の制御を行う制御部400と、制御データ及び制御手順等を記憶する記憶部401と、キー入力を行うキーパッド402と、表示出力をを行うディスプレイ403と、着信音等を出力するサウンド404と、これら入出力部と制御部との間のインターフェース部405と、無線回路部406と、ベースバンド処理部407、マイク408と、スピーカ409を有して構成される。

【0050】次に、図15のP H S端末のブロック図と図16、17のP H S送信部／受信部のフローチャートを参照して処理手順について説明する。P H S端末は、図14のベースバンド処理部407に対応するリニアコーデック処理部510と、音声符号化／復号化部511と、音声／32k b p sデータ切替部512と、暗号化／復号化部513と、チャネルコーデック処理部514と、モデム処理部515と、図14の無線回路部406に対応する無線回路部516を有して構成される。送信部は、まず、ステップ600において、伝送したい音声／32k b p sデータを入力する。次に、ステップ601において、音声／32k b p sデータ切替部512で音声データがP H S端末に入力されるか判定を行う。音声データが入力されるならばステップ602以降の処理を行い、32k b p sデータが入力されるならばステップ604以降の処理を行う。次に、ステップ602において、ディジタル処理を行うために、入力された300～3400Hzのアナログ音声信号をリニアコーデック処理部510で64k b p sのディジタル信号に変換する。次に、ステップ603において、音声符号化／復号化部411で音声符号化処理を行い、64k b p sのP CMデータを32k b p sの音声符号化ビットに変換する。次に、ステップ604において、暗号化／復号化処理部513で前記音声符号化データやF A X、パソコン等の各種データに対して、任意のビット長だけ格納し、そのビット長を1ブロックとして任意の暗号化アルゴリズムで暗号化処理を行う。次に、ステップ605において、チャネルコーデック処理部514で暗号化されたビットをあるブロック（P H Sの場合データ160ビット）毎に格納し、そのブロックごとに巡回符号（C R C）による符号化を行い、データ160ビットに符号化されたビットを付け加えるチャネルコーデック処理を行う。次に、ステップ606において、モデム処理部515でチャネルコーデック処理によって出力された送信データのディジタル変調（P H Sの場合はπ/4シフトQ P S K）を行う。次に、ステップ607において、無線回路部516で無線チャネルの設定を行い、音声や各種データを無線回線を使って伝送することができる。以上

の処理によって、音声や各種データを無線回線を使って送信することができる。

【0051】受信時の動作を以下に説明する。受信部では、まずステップ700において無線回路部516で無線チャネルから伝送されてきた信号を受け取る。次に、ステップ701において、モデム処理部515で信号の復調処理を行う。次に、ステップ702において、チャネルコーデック処理部514で送信部と同じように復調処理を行ったビットに対して、あるブロック(PHSの場合はデータ160ビット)毎に、巡回符号(CRC)による符号化を行い、送信部から伝送されてきた巡回符号(CRC)による符号化ビットと比較し、伝送路での誤り検出を行う。次に、ステップ703において、伝送路での誤りが検出されたかどうかの判定を行う。誤りが検出されればステップ704の処理を行い、誤りが検出されなければステップ705の処理を行う。次に、ステップ704において、誤り除去又は低減処理を行う。次に、ステップ705において、暗号化/復号化処理部513で情報ビット(PHSの場合は160ビット)に対して、任意のビット長だけ格納し、そのビット長を1ブロックとして任意の復号化アルゴリズムで復号化処理を行う。次に、ステップ706において、音声/32kbpsデータ切替部512で音声データであるか判定を行う。音声データであればステップ705へ、32kbpsデータであればステップ708の処理を行う。次に、ステップ707において、音声符号化/復号化部511で音声復号化処理を行い、32kbpsの音声符号化データを64kbpsのPCMデータに変換する。次に、ステップ708において、アナログ信号を得るために(音声を出力するため)、リニアコーデック処理部510で64kbpsのデジタル信号を300~3400Hzのアナログ音声に変換する。次に、ステップ707において、スピーカ402等の手段を通して、音声を出力する。また、ステップ708において、FAX、パソコン等の32kbpsデータ503を出力する。以上の処理によって、無線回線から音声や各種データを受信することができる。

【0052】また、図15のPHS端末ブロック図中の暗号化/復号化部513の中の暗号化部の従来例について図18に示し、図19の暗号化部の処理手順と合わせて従来の暗号化部について説明する。

【0053】暗号化部は、メッセージ格納バッファ1010と、暗号化アルゴリズム格納部1011と暗号化処理部1012を有して構成される。まず、ステップ100において、メッセージ1000(音声符号化ビット)を入力する。次に、ステップ1101において、暗号化アルゴリズムの処理ビット数に応じたメッセージを1ブロックとしてメッセージ格納バッファ1010に格納する。次に、ステップ1102において、1ブロック毎に暗号化アルゴリズム格納部1011に格納してある

暗号化アルゴリズムに基づき暗号化処理を行う。次に、ステップ1103において、暗号文1001が出力される。以上の処理によって、メッセージの暗号化が行われる。

【0054】これに対して、図15のPHS端末ブロック図の暗号化/復号化部513の中の復号化部の従来例を図20に示し、図21の復号化部の処理手順と合わせて従来の復号化部について説明する。

【0055】復号化部は、暗号文格納バッファ1210と、復号化アルゴリズム格納部1211と、復号化処理部1212を有して構成される。まず、ステップ1300において、暗号文を入力する。次に、ステップ1301において、復号化アルゴリズムの処理ビット数に応じて、暗号文数ビットを1ブロックとして暗号文格納バッファ1210に格納する。次に、ステップ1302において、1ブロック毎に復号化アルゴリズム格納部に格納してある復号化アルゴリズムに基づき復号化処理を行う。次に、ステップ1303において、メッセージ1201が出力される。以上の処理によって、暗号文の復号化が行われる。

【0056】図22は、本発明にかかる暗号化部即ち暗号化処理を行う手段の構成図である。

【0057】暗号化処理は、メッセージ格納バッファ1410と、暗号化アルゴリズム格納部1411-1~1411-Nと、暗号化アルゴリズム切替部1412と、暗号化アルゴリズム識別子決定部1413と、暗号化処理部1414と、識別子暗号化処理部1415と、送信データ格納部1416を有して構成される。メッセージ格納バッファ1410は、暗号化アルゴリズムの処理ビット数に応じて、メッセージ1400を格納するバッファである。暗号化アルゴリズム格納部1411-1~1411-Nは、複数の暗号化アルゴリズムを全て備えていて、暗号化処理部1414からの命令に応じ暗号化アルゴリズムを呼び出すときに使われる手段である。暗号化アルゴリズム切替部1412は、盗聴防止のため、端末ユーザーの暗号化アルゴリズム変更要求時に、キー入力等の手段によって任意に又は呼接続時毎に、位置登録時毎に、通話中チャネル切り替え時毎に、認証時毎に、予め定められた時間毎に、全くランダムな時間毎に、予め定められたエリア毎に端末が暗号化アルゴリズムを切り替える手段である。暗号化アルゴリズムを切り替える手段の一例としては、暗号化装置が、図4に示すように複数の暗号化アルゴリズムと対応する暗号化アルゴリズム識別子をメモリ等の手段に格納していて、CPU等の手段が暗号化アルゴリズム識別子のビット数に対応する乱数を任意の乱数発生器で出し、出力された乱数を用い図14に示すような対応表から暗号化アルゴリズムを選択し、暗号化アルゴリズムを切り替える。暗号化アルゴリズム識別子決定部1413は、決定された暗号化アルゴリズムの識別子を出力する手段である。暗号化処理部

1414は、切り替えられ選択された暗号化アルゴリズムによって、メッセージを暗号化し、暗号文1402を出力する手段である。識別子暗号化処理部1415は、前記暗号化アルゴリズム識別子を任意の暗号化アルゴリズムで暗号化を行い、識別子暗号文を出力する手段である。送信データ格納部1416は、前記識別子暗号文1403と、前記暗号文1402を並べて同時に格納する手段である。

【0058】ここで、対応する暗号化部の処理手順を図23に示し、該フローチャートを参照して処理手順について説明する。

【0059】まず、ステップ1510において、ユーザがキー入力で任意に暗号化アルゴリズムの変更をできるように設定するか判定を行う。もし、設定するならばステップ1212の処理を行い、設定しなければステップ1511の処理を行う。次に、ステップ1511において、盜聴防止のため、呼接続時毎に、位置登録時に、通話中チャネル切り替え時毎に、認証時毎に、予め定められた時間毎に、全くランダムな時間毎に、予め定められたエリア毎に端末が暗号化アルゴリズムを変更できるように設定するか判定を行う。もし設定するならば、ステップ1514の処理を行い、設定しなければ、ステップ1515の処理を行う。

【0060】次に、ステップ1512において、ユーザがキー入力で暗号化アルゴリズムの変更を要求しているか判定を行う。もし変更を要求していれば、ステップ1514の処理を行い、変更を要求していないければステップ1513の処理を行う。次に、ステップ1513において、呼接続時又は位置登録時又は通話中チャネル切り替え時又は認証時又は予め定められた時間又は端末がエリア変更を行ったか判定を行う。1つでもあてはまるば、ステップ1514の処理を行い、1つもあてはまらなければ、ステップ1515の処理を行う。次に、ステップ1514において、暗号化アルゴリズム識別子のビット数に対応する乱数を任意の乱数発生器で出力し、図4に示すような対応表から暗号化アルゴリズムを決定する。なお、図4の識別子は、3ビットで示しているが、ビット数は任意で良い。ステップ1515においては、以前に使っていた暗号化アルゴリズムを使用する。同様に、以前に使っていた暗号化アルゴリズム識別子を使用する。次に、ステップ1516において、暗号化アルゴリズム識別子を任意の暗号化アルゴリズムで暗号化し、識別子暗号文1503を出力する。次に、ステップ1517において、暗号化処理の入力に応じて、メッセージ1500の数ビットを1ブロックとして格納する。次に、ステップ1518において、1ブロック毎に暗号化アルゴリズムに基づき暗号化処理を行い、暗号文を前記バッファへ出力する。次に、ステップ1519において、前記バッファに格納された暗号文と識別子暗号文を通信用物理スロットを使って同時に伝送路へ送る。

【0061】以上の処理によって、メッセージの暗号化が行われ、バッファへ出力された暗号文と識別子暗号文は、同時に伝送される。

【0062】これに対して、図24は、本発明にかかる実施例における、暗号文の復号化処理を行う手段の構成図である。

【0063】復号化処理は、受信データ分割部1610と、識別子復号化処理部1611と、復号化アルゴリズム選択部1612と、復号化アルゴリズム格納部1613-1～1613-Nと、復号化アルゴリズム切替部1614と、暗号文格納バッファ1615と、復号化処理部1616を有して構成される。受信データ分割部1610は、受信したデータを識別子暗号文1600と暗号文1601に分割する手段である。識別子復号化処理部1611は、前記識別子暗号文1600の復号化を行い、暗号化アルゴリズム識別子を出力する手段である。

復号化アルゴリズム選択部1612は、暗号化アルゴリズム識別子から図4に示すような対応表から復号化アルゴリズムを選定する手段である。復号化アルゴリズム格納部1613-1～1613-Nは、複数の復号化アルゴリズムを全て備えていて、復号化処理部1616の命令に応じ復号化アルゴリズムを呼び出すときに使われる。復号化アルゴリズム切替部1614は、復号化アルゴリズムを切り替える手段である。復号化処理部1616は、切り替えられた復号化アルゴリズムによって、メッセージ1603を復号化する手段である。

【0064】ここで、対応する復号化部の処理手順を図25に示し、該フローチャートを参照して処理手順について説明する。

【0065】まず、ステップ1710において、復号化部が処理開始可能なスタンバイ状態であることを確認する。スタンバイ状態であれば、ステップ1711の処理を行い、スタンバイ状態でなければ、ステップ1710の処理を繰り返す。次に、ステップ1711において、受信したデータを暗号文と識別子暗号文に分割する。暗号文はステップ1715以降で使われ、識別子暗号文はステップ1712以降で使われる。次に、ステップ1712において、前記識別子暗号文を任意の復号化アルゴリズムで復号化し、暗号化アルゴリズム識別子を出力する。次に、1713において、前記暗号化アルゴリズム識別子に基づいて、図10に示すような対応表から復号化アルゴリズムを選びだす。次に、ステップ1714において、選びだされた復号化アルゴリズムに切り替える。次に、ステップ1715において、復号化処理の入力に応じて、暗号文数ビットを1ブロックとして格納する。次に、ステップ1716において、1ブロック毎に復号化アルゴリズムに基づき復号化処理を行い、メッセージを出力する。

【0066】以上の処理によって、暗号文の復号化が行われる。

【0067】ここで、送信側から受信側への暗号化アルゴリズム識別子の伝送手段を説明する。

【0068】暗号化アルゴリズム識別子は、端末ユーザの暗号化アルゴリズム変更要求時にキー入力で又は呼接続時毎、位置登録時毎、通話中チャネル切り替え時毎、認証時毎、予め定められた時間毎、全くランダムな時間毎、予め定められたエリア毎に暗号化アルゴリズムを変更するように設定した場合、暗号化アルゴリズムを変更する毎に送信側から受信側へ伝送する必要がある。

【0069】呼接続時は、通話開始時のこととし、呼接続毎に暗号化アルゴリズムを変更するように設定した場合、通話開始後すぐに暗号化アルゴリズム識別子を伝送する。位置登録は、移動局が基地局へ新たに位置登録を要求するために行うものである。位置登録時毎に暗号化アルゴリズムを変更するように設定した場合、位置登録終了後すぐに暗号化アルゴリズム識別子を伝送する。通話中チャネル切り替えは、ユーザがチャネル切り替えを要求した場合、又は受信レベルが劣化したり、受信品質が劣化した場合他のチャネルへ切り替えるものであり、ハンドオーバーも含まれる。通話中チャネル切り替え時毎に暗号化アルゴリズムを変更するように設定した場合、チャネル切り替え終了後すぐに暗号化アルゴリズム識別子を伝送する。認証時は、呼接続時、位置登録時、通話中チャネル切り替え時毎に基地局が移動局の正当性を確認するために行う。認証時毎に暗号化アルゴリズムを変更するように設定した場合、通話開始後すぐに暗号化アルゴリズム識別子を伝送する。予めフレーム

(5 ms) 每又は1時間毎に暗号化アルゴリズムを変更するように設定した場合、暗号化アルゴリズム変更とともに暗号化アルゴリズム識別子を伝送する。全くランダムな時間毎に暗号化アルゴリズムを変更するとは、乱数発生器の出力の値をランダムな時間と考え、そのランダムな時間毎に暗号化アルゴリズムを変更することを示す。この場合も暗号化アルゴリズム変更とともに暗号化アルゴリズム識別子を伝送する。

【0070】暗号化アルゴリズム識別子を伝送する一例を以下に述べる。図26は、本発明にかかる、低速付随チャネル(以下SACCHという。)を使って暗号化アルゴリズム識別子を伝送する手段の通信用物理スロットの例を示す。図26の暗号通信の可能な通信用物理スロットの例を示す。Rは信号の過渡応答を保護するための過渡応答用ランプタイム領域であり、SSはフレームの信号を知らせるスタートシンボル領域であり、PRはビット同期確立のためのプリアンブル領域であり、UWは制御用物理スロットと通信用物理スロットを区別するための同期ワード領域であり、CIはチャネルの種別を規定するチャネル種別領域であり、SAは制御情報領域と該制御情報領域内に格納される情報の種類の識別符号である識別符号領域とから構成されるSACCH領域であり、TCHは伝送すべき情報を格納すべき情報を格納す

る情報チャネル領域であり、CRCは誤り検出用巡回符号領域であり、ガードビット領域は送信バースト信号が隣接するスロット間で相互に衝突しないようにバースト信号間に用意する無信号時間である。上記制御情報領域内に格納される情報は暗号化及び復号化の同期確保用情報出ある。

【0071】暗号化及び復号化間の同期確保用の暗号化情報領域と、伝送すべき情報を格納する情報チャネル領域と、通話中、SACCHを使用するのは、位置登録、チャネル切り替えの時であり、それ以外では使用されていない。よって、使用されていない時に、暗号化アルゴリズム識別子をSACCHを使って暗号化側から復号化側へ伝送すれば、同期はずれを防止できる。

【0072】ここで、対応する暗号化アルゴリズム識別子の送信手順を図27に示し、該フローチャートを参照して処理手順について説明する。まず、ステップ1900で低速付随チャネルが使用可能な状態であるか判定を行う。使用可能な状態は、SACCHの先頭ビットが2スロット連続で1の場合であり、使用不可能な状態はSACCHの先頭ビットが1スロット目が0で、2スロット目が1の場合である。もし、使用可能な状態であればステップ1901の処理を行い、使用不可能な状態であればステップ1904の処理を行う。ステップ1901で暗号化アルゴリズム識別子を伝送していることを示す識別子を付ける。識別子は、SACCHの先頭ビットが2スロット連続で0の場合とする。次に、ステップ1902で、暗号化アルゴリズム識別子をSACCHの情報フィールドに入力する。ステップ1903では、そのフレームに関して暗号化アルゴリズム識別子の伝送を行わない。

【0073】また、暗号化アルゴリズム識別子の受信手順を図28に示し、該フローチャートを参照して、処理手順について説明する。まず、ステップ2000で、SACCHが暗号化アルゴリズム識別子情報であるかを判定する。暗号化アルゴリズム識別子情報である場合は、SACCHの先頭ビットが2スロット連続で0の場合であり、それ以外の場合は暗号化アルゴリズム識別子情報でない。暗号化アルゴリズム識別子情報でない場合はステップ2002の処理を行い、暗号化アルゴリズム識別子の場合は、ステップ2001の処理を行う。ステップ2001では、SACCHの情報フィールドから暗号化アルゴリズム識別子を受け取る。ステップ2002では、SACCHの情報フィールドから暗号化アルゴリズム識別子を受け取らない。以上の処理によって、SACCH使用可能なときのみ、暗号化アルゴリズム識別子の送受信を行うことができる。

【0074】今後新しい暗号化アルゴリズムが開発され、その新しい暗号化アルゴリズムを備えた特定の端末と基地局間、又は特定の端末間だけしか情報の送受信を行うことができなくなるという課題を解決するために次

のような着脱式メモリシステムを利用した暗号化／復号化装置の構成図を図29及び図1に示し、該構成図を参照して実施例を説明する。

【0075】本発明による着脱式メモリシステムは、各種端末機器2110と、着脱式メモリ読取り装置2111と、着脱式メモリ2112を有して構成される。

【0076】なお、着脱式メモリ内部は、例えばDSP、CPU、ROM、RAM各種CMOS等の一般的な電子デバイスにて構成される。

【0077】各種端末機器2110としては、パーソナルコンピュータ・自動取引装置(ATM)やPHS端末など応用分野のニーズに対応した各種の装置が開発されている。

【0078】着脱式メモリ読取り装置2111は、着脱式メモリ2112の動作に必要な電源2100、クロック等の制御信号2101を供給し、データ2102の送受信の制御を行うユニットであり、各種端末機器あるいはホストシステムに接続することができてもよい。

【0079】着脱式メモリ2112の例としては、RAMあるいはROM等の素子を高密度実装技術により内蔵したものである。また、読み取り装置はマイクロコンピュータの制御プログラムの管理下で装着部に設けられた接点を通して外部装置との情報交換を行う。着脱式メモリに内蔵されたメモリ2122は、データ保護のため、一定の手順で処理が行われた場合のみアクセスされるよう制御されている。

【0080】ここで、本発明の着脱式メモリシステムの処理手順を図30に示し、該フローチャートを参照して、処理手順について説明する。

【0081】まず、ステップ2200において、着脱式メモリを各種端末機器に接続された着脱式メモリ読取り装置に差し込む。次に、ステップ2201において、着脱式メモリ読取り装置を通じ、着脱式メモリに電源、クロック、制御信号が供給される。次に、ステップ2202において、あらかじめ決められたプロトコルに基づきメモリに格納されている暗号化アルゴリズムを読み取る。

【0082】以上の処理によって、各種端末機器に接続された着脱式メモリ読取り装置が、着脱式メモリ上の接点を通じて情報のやりとりを行う。

【0083】図31は、本発明の着脱式メモリシステムを利用した暗号化装置の実施例であり、着脱式メモリのリード／ライトを行う着脱式メモリ読取り装置用のスロットを持つ暗号化／復号化装置を備えたPHS端末を示す。

【0084】本発明によるPHS端末は、PHS端末本体2300と、着脱式メモリ読取り装置2301と、着脱式メモリ2302を有して構成される。

【0085】PHS端末本体2300は、音声データやFAX、パソコン等の各種データを送信したり、受信し

たりする端末のこと、暗号化アルゴリズム識別子から暗号化アルゴリズムをディスプレイ等の手段に表示する機能を有し、図13のような構成になっている。着脱式メモリ読取り装置2301は、着脱式メモリ2302の動作に必要な電源、クロック、等の制御信号を供給し、データのリード／ライトを行う手段であり、標準インターフェース等を経由して、PHS端末本体に接続する手段である。着脱式メモリ2302は、メモリ等の素子を高密度実装技術により一体化したもので、メモリ素子の中に今後新たに開発される暗号化アルゴリズムと復号化アルゴリズムと暗号化アルゴリズムを識別する暗号化アルゴリズム識別子を備えていて、マイクロコンピュータの制御プログラムの管理下で着脱式メモリ2302の表面に設けられた接点を通して、PHS端末本体との情報交換を行う手段である。

【0086】図32のように、暗号化装置を備えた既存端末に対して基地局側に本発明の復号化装置を設けることによって、既存端末側で暗号化アルゴリズムを識別するための暗号化アルゴリズム識別子を付加し、基地局側の基地局1の復号化アルゴリズム格納部に格納されている復号化アルゴリズムに対応する暗号化アルゴリズムで暗号化を行えば、既存端末からの情報を受信することができる。逆に基地局側に本発明の暗号化装置を設けることによって、既存端末の復号化アルゴリズムに対応する暗号化アルゴリズムで暗号化を行えば、本発明の基地局側からの情報を既存端末に送信することができる。

【0087】また、図33のように、既存基地局に対して、端末側に本発明の暗号化装置を設けることによって、既存基地局の復号化アルゴリズムに対応する暗号化アルゴリズムで暗号化を行えば、本発明の端末側からの情報を既存基地局に送信することができる。逆に既存基地局に対して端末側に本発明の復号化装置を設けることによって、既存基地局で暗号化アルゴリズムを識別するための暗号化アルゴリズムを付加し、端末側のPHS端末1の復号化アルゴリズム格納部に格納されている復号化アルゴリズムに対応する暗号化アルゴリズムで暗号化を行えば、既存基地局からの情報を受信できる。

【0088】また、図34のように、端末側に本発明の暗号化装置を基地局側に本発明の復号化装置を設けることによって、端末側で暗号化アルゴリズムを識別するための識別子を付加するだけで、暗号化アルゴリズム格納部に格納されている暗号化アルゴリズムのいずれかで暗号化を行えば、情報を端末側から基地局側に送信することができる。逆に、端末側に本発明の復号化装置を基地局側に本発明の暗号化装置を設けることによって、基地局側で暗号化アルゴリズムを識別するための識別子を付加するだけで、暗号化アルゴリズム格納部に格納されている暗号化アルゴリズムのいずれかで暗号化を行えば、情報を基地局側から端末側に送信することができる。

【0089】また、今後新たに開発される暗号化アルゴ

リズムを備えた着脱式メモリを使用した場合も、復号化側で暗号化アルゴリズム識別子をディスプレイ等に表示して、表示したとおりの着脱式メモリを差せば、任意の端末間で情報の伝送を行うことができる。

【0090】次に図35に示した本発明における基地局及び管理局について説明する。本発明の無線基地局では、メモリ等からなる記憶部に複数の暗号化／復号化アルゴリズムと、それに対応する識別子、あるいは、ある暗号化から他の暗号化へ直接変換できる暗号化変換アルゴリズムを有している。また、暗号化／復号化アルゴリズム及び暗号化変換アルゴリズムと／＼に対応する識別子との関係を表すテーブルを記憶するものであってよい。一方、管理局では複数の無線基地局をその管理下に置いている。

【0091】ここで、従来の問題点を簡単に説明すると、新しい暗号化アルゴリズムが採用されることになった場合、従来は新しい暗号化アルゴリズムを備えた新しい無線通信端末及び無線基地局等が必要となっていたため、コスト的に大変不利であった。また、インフラの再整備には莫大な費用がかかるため、折角、強力な暗号化アルゴリズムが作られても使用することが困難であった。

【0092】そこで、この問題を解決する第1の構成として本発明の無線基地局では図9～12に示したように記憶部が着脱可能（着脱部の構成は図1の無線通信端末と同様に、読み取り部、装着部、着脱交換記憶装置からなる）であるため容易かつ安価に新しい暗号化／復号化アルゴリズムに対応できる。

【0093】第2の構成として図35に示すようには、無線基地局(CS)を管理する管理局のみを新しい暗号化／復号化アルゴリズムに交換しさえすれば、管理局に通信回線で接続された無線基地局の記憶部に反映される構成となっている。

【0094】ここで無線基地局の記憶部が更新される手順を説明する。まず、管理局の記憶部に新しい暗号化／復号化アルゴリズムを登録する。次に、管理局の支配下に存在する無線基地局に対して、制御部に制御された回線インターフェースは回線接続する。回線接続したのち管理局の制御部は無線基地局に対して、無線基地局の記憶部に記憶されている暗号化／復号化テーブルの更新を命令する命令信号を発する。命令信号を受けた無線基地局では、管理局が通信回線を介して送信してくる暗号化／復号化アルゴリズム及び識別子、暗号化テーブル等を受信し記憶部を更新する。

【0095】次に図37から40に示した本発明の通信システムについて説明する。

【0096】図37に示す通信システムは、暗号化／復号化アルゴリズムAのみを有する無線通信端末(PS1)と暗号化／復号化アルゴリズムBのみを有する無線通信端末(PS2)とが本発明の無線基地局(CS1)を介すことによっ

て通信する図を示す。本来であればPS1とPS2とでは暗号化／復号化アルゴリズムが異なっているため直接通信不可能であるが、無線基地局CS1が複数のアルゴリズムを備え、かつ、呼接続時に発呼者側と着呼者側とが備えている暗号化／復号化アルゴリズムの種類を問い合わせるか、あるいはデータベースから無線通信端末の保有する暗号化／復号化アルゴリズム情報を検索することで、適切な呼接続を行うことができる。このデータベースは位置登録情報などのデータベースを利用すれば安価に構成できよう。

【0097】また、無線基地局は暗号化／復号化アルゴリズムをAからBへ直接変換することができる暗号化変換アルゴリズムを備えてもよい。これを用いれば、高速に変換ができる。

【0098】図38に示した本発明の通信システムでは本発明の無線通信端末と、既存の、あるいは最新の暗号化／復号化アルゴリズムに一部対応できない無線基地局を介す場合をしめす。

【0099】既存の無線基地局は暗号化に対応していないため暗号化が施されたまま通信データを素通しにする。この場合本発明の無線通信端末では、通信中に相手方の保有する暗号化／復号化アルゴリズムと自局の有するもののうち共通のものうちの何れかによって暗号化通信を行うよう設定する。呼接続時あるいは呼接続後に確認された共通の暗号化／復号化アルゴリズムを用いて、図23のフローチャートに従って暗号化／復号化アルゴリズムを変化させながら通信すればより強力な暗号通信が行えよう。

【0100】図39に示した本発明の通信システムでは、複数の無線基地局を介して通信する場合を示している。本発明の無線基地局(CS3, CS4)を介すことにより全ての暗号化／復号化アルゴリズムに対応していない無線通信端末であっても、本発明の無線基地局が全ての暗号化／復号化アルゴリズムに対応しているため何の支障もなく暗号通信が可能となる。

【0101】図40に示した本発明の通信システムでは、無線基地局が全ての暗号化／復号化アルゴリズムに対応できていない場合であっても本発明の無線通信端末を用い、さらに、この無線通信端末間で暗号化／復号化アルゴリズムをハンドシェークすることによって双方の無線区間で暗号化通信が可能となる。

【0102】次に本発明の無線通信端末を図41、42、43を用いて説明する。本発明の無線通信端末では、本発明の暗号化／復号化アルゴリズムなどを記憶した着脱交換式のカード型メモリを装着するための装着部4102、4202、4302を備えたものである。これにより、無線通信端末の筐体4101、4201、4301を開くことなく閉じたままで、容易に新たな暗号化／復号化アルゴリズムを記憶したカード型メモリを交換できるものである。これによって、専門の知識を特に

有しないユーザなどであっても、容易に交換できるため、交換サービスをメーカや通信サービス会社が行うことを省略できるため、サービス面でのコストが大幅に削減できる。

【0103】また、図43のようにカード型メモリの装着部に安全のために蓋を設けると良い。これによって装着部から筐体内部へほこりや水滴の進入を防ぐことができるとともに、カード型メモリを保護し、外れて落下することも防止できる。

【0104】

【発明の効果】本発明によれば、暗号化アルゴリズムを端末ユーザーの暗号化アルゴリズム変更要求時にキー入力等の手段によって任意に又は呼接続時毎に、位置登録時毎に、通話中チャネル切り替え時毎に、認証時毎に、予め定められた時間毎に、全くランダムな時間毎に、予め定められたエリア毎に、端末が切り替えるという設定を複数行えば、解読されにくい強力な暗号化を行うことができる。又、送信側で暗号化アルゴリズム識別子を付加するだけで、暗号化アルゴリズム格納部1411-1～1411-Nに格納されている暗号化アルゴリズムのいずれかで暗号化を行い、受信側で前記暗号化アルゴリズム識別子を基に復号化アルゴリズム格納部1612-1～1612-Nに格納されている復号化アルゴリズムのいずれかで復号化を行えば、任意の端末間で情報の伝送を行うことができる。又、送信側／受信側で同じ暗号アルゴリズムを備えた着脱式メモリを使用することで、任意の端末間で情報の伝送を行うことができる。つまり、このような暗号化／復号化装置を使うことで、自社、他社を問わずどの端末を使っても音声や様々なデータの通信を行うことができる。

【図面の簡単な説明】

- 【図1】本発明の無線通信端末を示す図。
- 【図2】本発明の端末の送信部を示す図。
- 【図3】本発明の端末の送信部を示す図。
- 【図4】識別子と暗号化アルゴリズムの対応の例を示す図。
- 【図5】本発明のPHS端末送信側のフローチャート図。
- 【図6】本発明の端末の受信部を示す図。
- 【図7】本発明の端末の受信部を示す図。
- 【図8】本発明のPHS端末受信側のフローチャート図。
- 【図9】本発明の基地局の送信部を示す図。
- 【図10】本発明の基地局の送信部を示す図。
- 【図11】本発明の基地局の受信部を示す図。
- 【図12】本発明の基地局の受信部を示す図。
- 【図13】PHSの構成図。
- 【図14】PHS端末機能図。
- 【図15】PHS端末のブロック図。
- 【図16】PHS端末送信側のフローチャート図。

【図17】PHS端末受信側のフローチャート図。

【図18】従来のPHSにおける暗号化部のブロック図。

【図19】従来のPHSにおける暗号化部のフローチャート図。

【図20】従来のPHSにおける復号化部のブロック図。

【図21】従来のPHSにおける復号化部のフローチャート図。

【図22】本発明の暗号化部のブロック図。

【図23】本発明の暗号化部のフローチャート図。

【図24】本発明の復号化部のブロック図。

【図25】本発明の復号化部のフローチャート図。

【図26】通信用物理スロットの例を示す図。

【図27】暗号化アルゴリズム識別子の伝送手順を示す図。

【図28】暗号化アルゴリズム識別子の受信手順を示す図。

【図29】着脱式メモリシステムの構成図。

【図30】本発明の着脱式メモリシステムを利用した暗号化／復号化装置のフローチャート図。

【図31】本発明の着脱式メモリシステムを利用したPHS端末を示す図。

【図32】本発明の暗号化／復号化装置の配置の例を示す図。

【図33】本発明の暗号化／復号化装置の配置の例を示す図。

【図34】本発明の暗号化／復号化装置の配置の例を示す図。

【図35】本発明の管理局と基地局を示す図。

【図36】本発明の管理局の構成図。

【図37】本発明の通信システムを示す図。

【図38】本発明の通信システムを示す図。

【図39】本発明の通信システムを示す図。

【図40】本発明の通信システムを示す図。

【図41】本発明の無線通信端末を示す図。

【図42】本発明の無線通信端末を示す図。

【図43】本発明の無線通信端末を示す図。

【符号の説明】

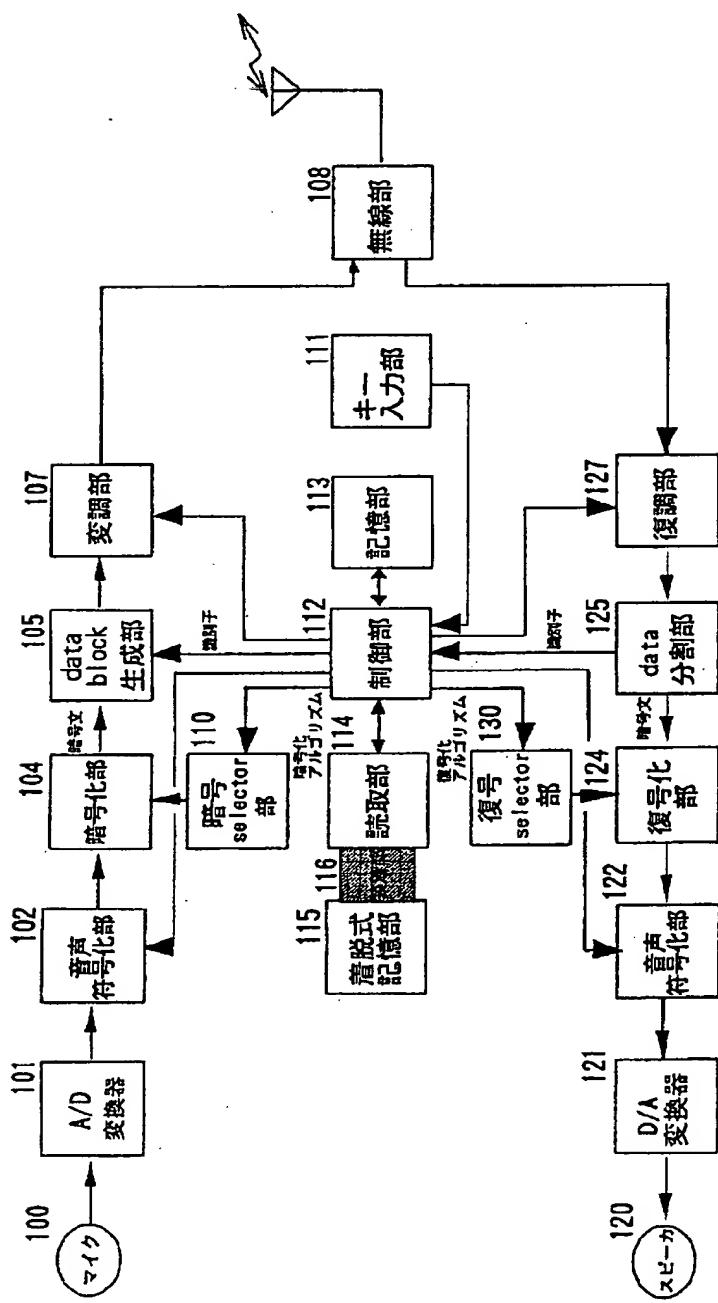
- 40 100…マイク、101…A/D変換器、102…音声符号化部、103…data selector部、104…暗号化部、105…data block生成部、106…誤り検出訂正符号化部、107…変調部、108…無線部、109…外部インタフェース部、110…暗号selector部、111…キー入力部、112…制御部、113…記憶部、114…読み取り部、115…着脱式記憶部、116…装着部、120…スピーカ、121…D/A変換器、122…音声復号化部、123…data判定部、124…復号化部、125…data分割部、126…誤

り検出訂正部、127…復調部、128…無線部、129…外部インターフェース部、130…復号 selector 部、131…キー入力部、132…制御部、133…記憶部、140…PBX、141…DSU、142…SINF、143…エコーキヤンセラ、144…音声符号化部、145…暗号化部、146…data block 生成部、147…誤り検出訂正符号化部、148…変調部、149…無線部、150

…暗号 selector 部、151…制御部、152…記憶部、160…PBX、161…DSU、162…SINF、163…エコーキヤンセラ、164…音声復号化部、165…復号化部、166…data 分割部、167…誤り検出訂正部、168…復調部、169…無線部、170…復号 selector 部、171…制御部、172…記憶部

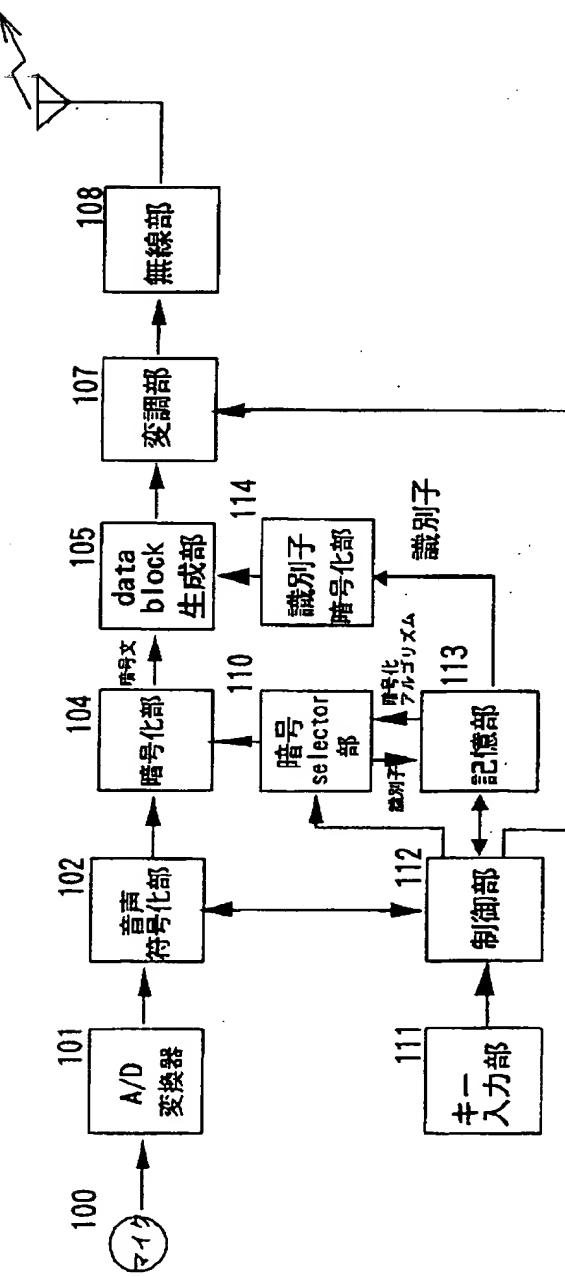
[図1]

図 1

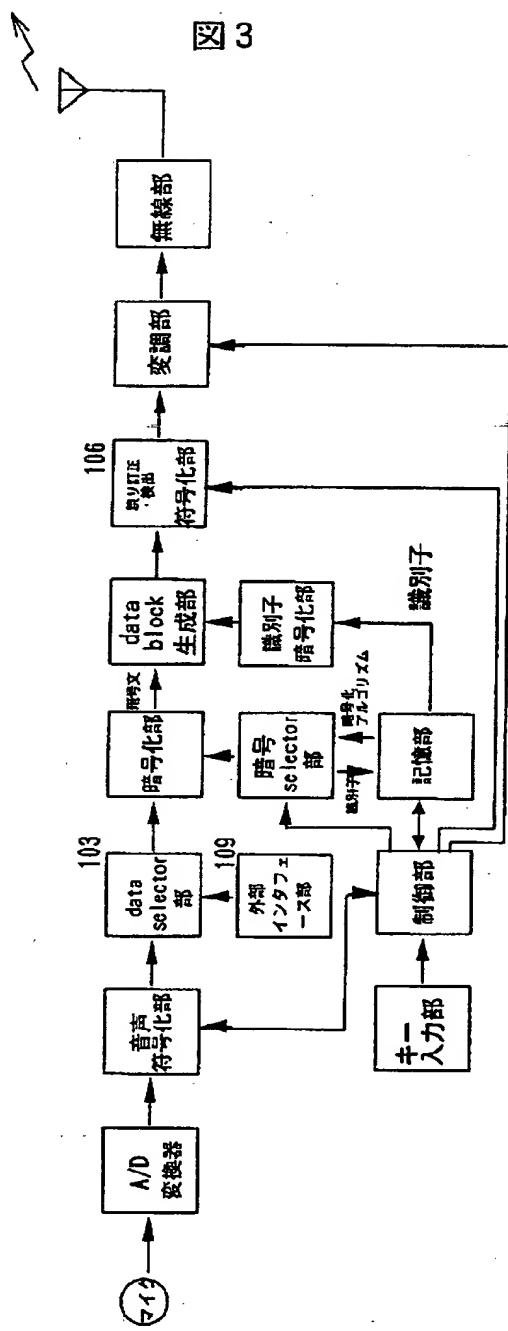


[図2]

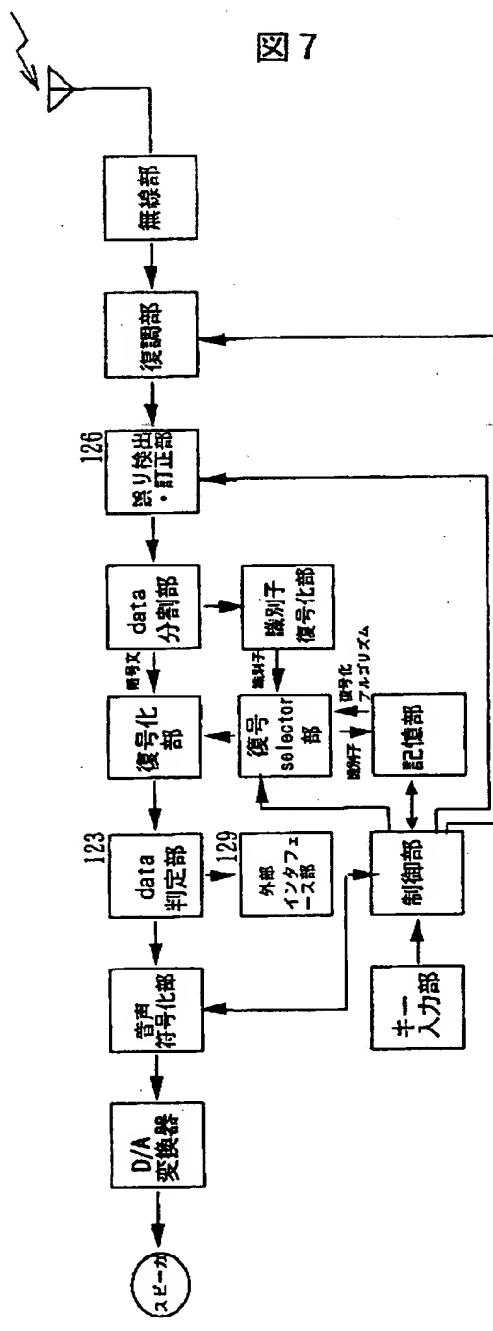
図 2



【図3】



【図7】



【図4】

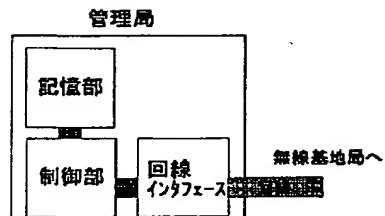
図4

番号子	暗号化アルゴリズム	復号化アルゴリズム
000	D	D ⁻¹
001	F	F ⁻¹
002	M	M ⁻¹
.	.	.
.	.	.
.	.	.

注) 復号化アルゴリズムの -1 は暗号化アルゴリズムの逆関数であることを示す。

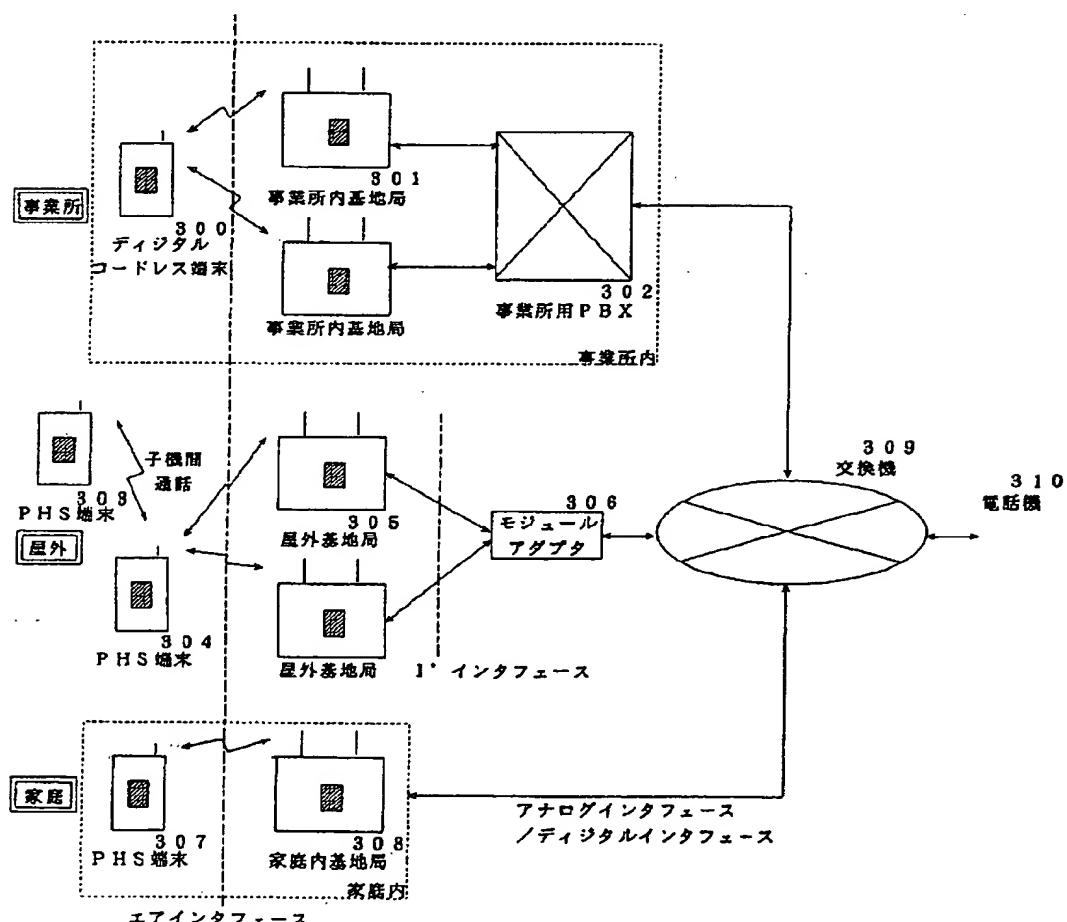
【図36】

図36



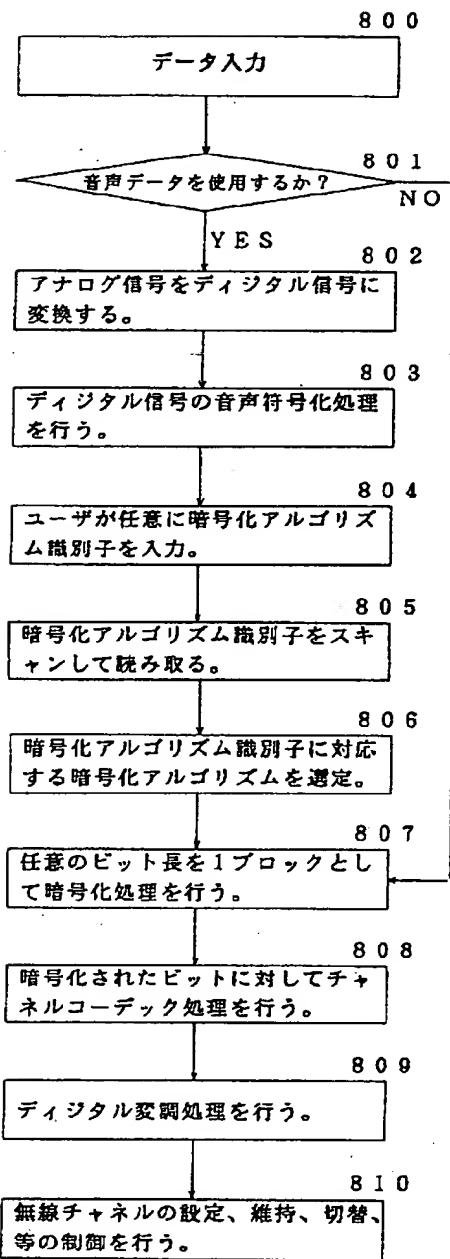
【図13】

図13



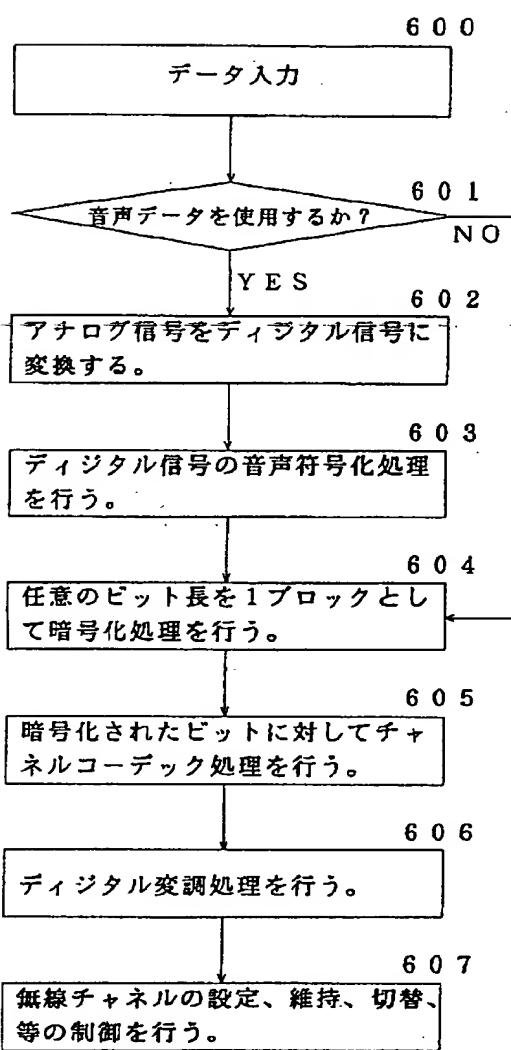
【図5】

図 5



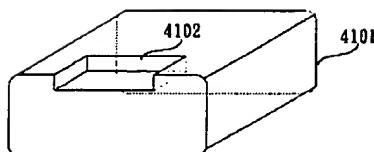
【図16】

図 16



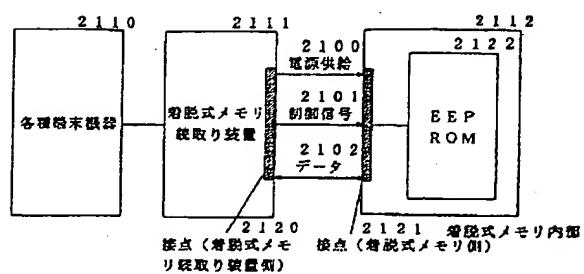
【図41】

図 41



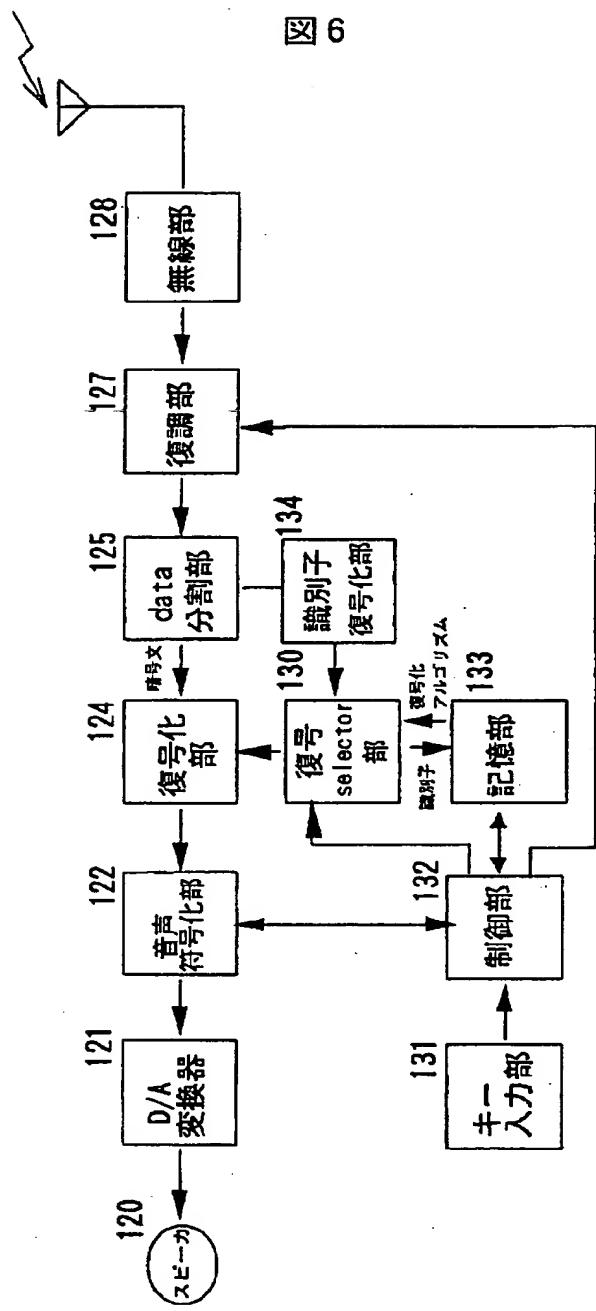
【図29】

図 29



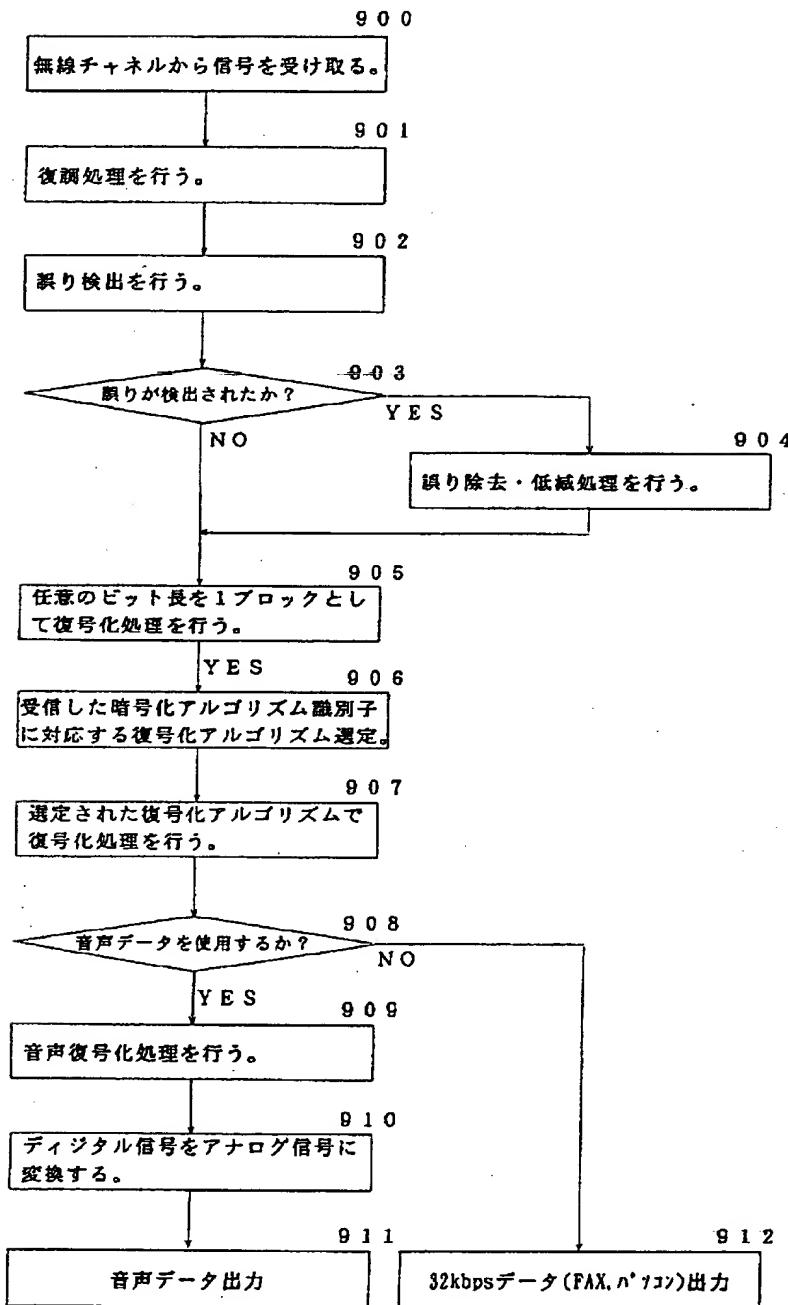
【図6】

図6



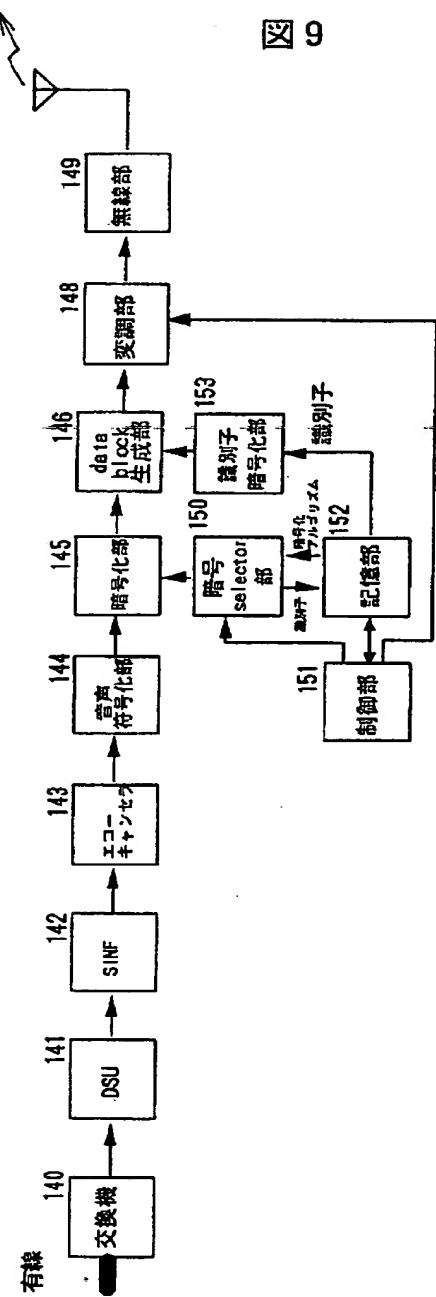
【図8】

図 8

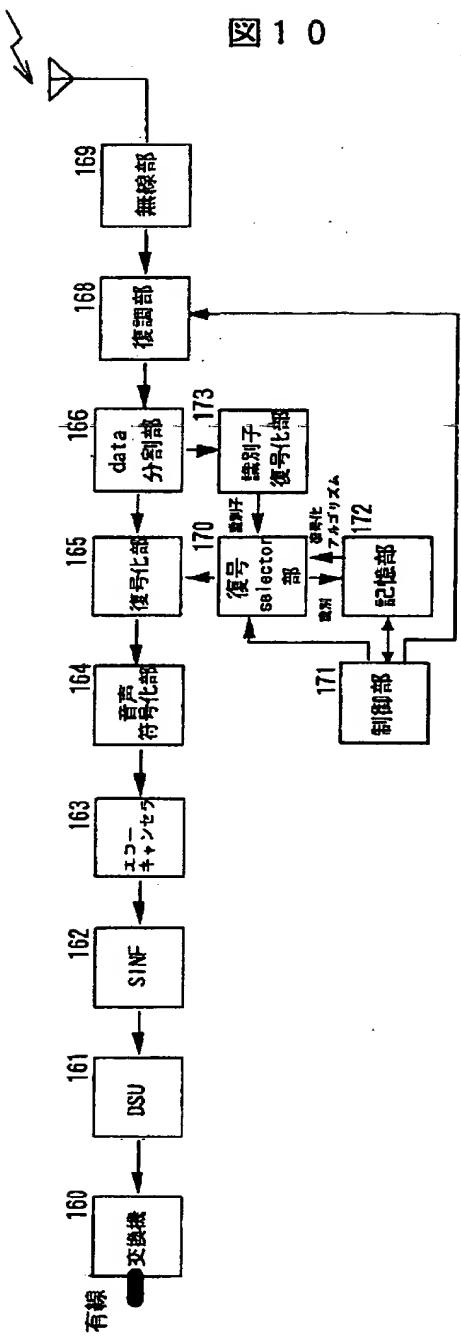


【図9】

図9

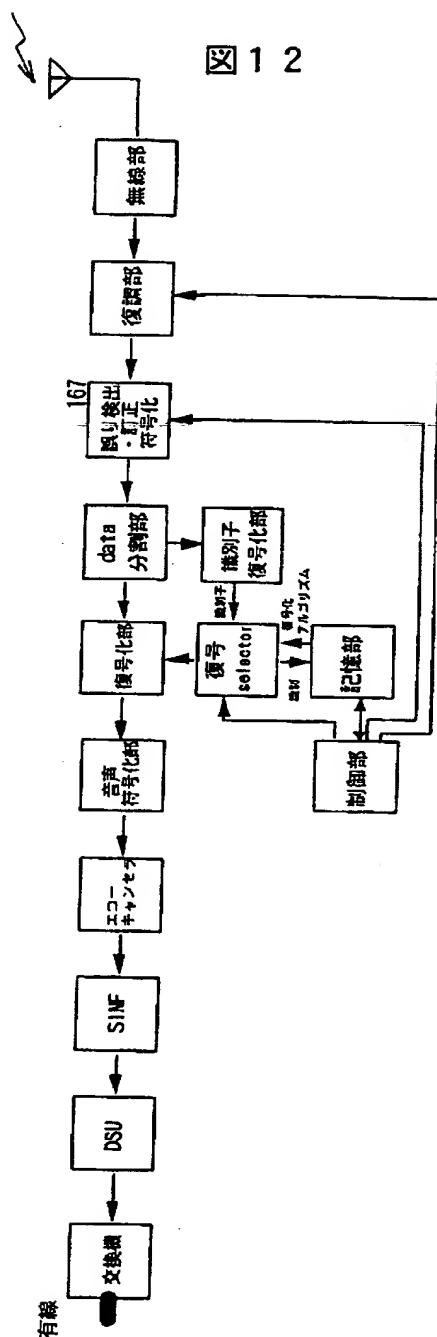


【図10】



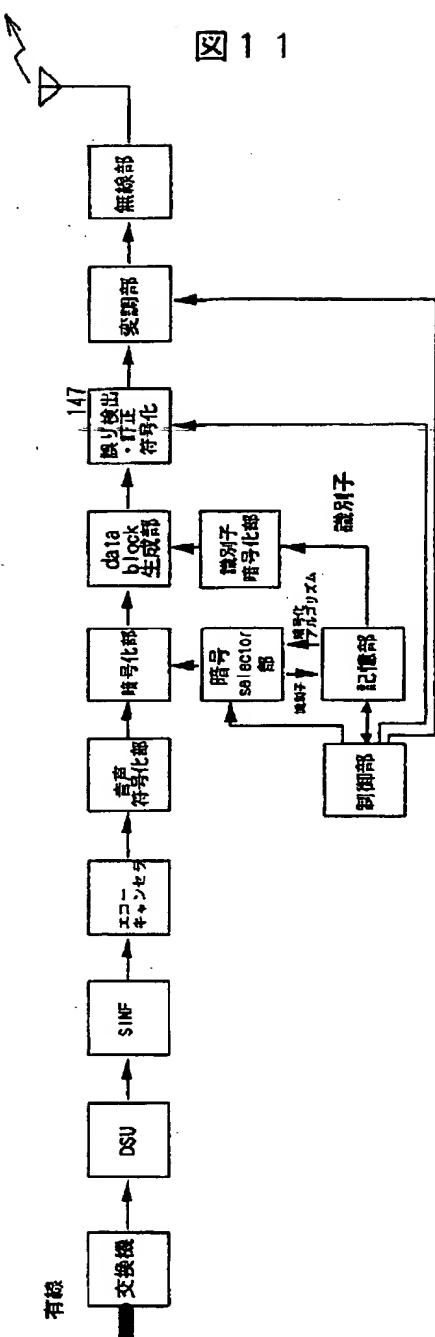
10

【図12】



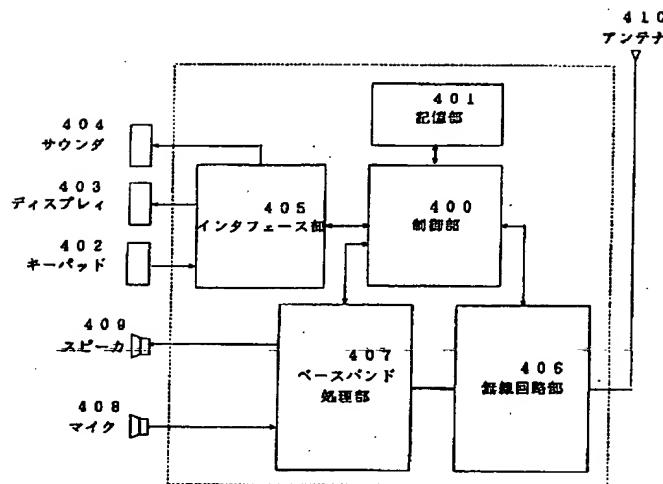
12

【図11】



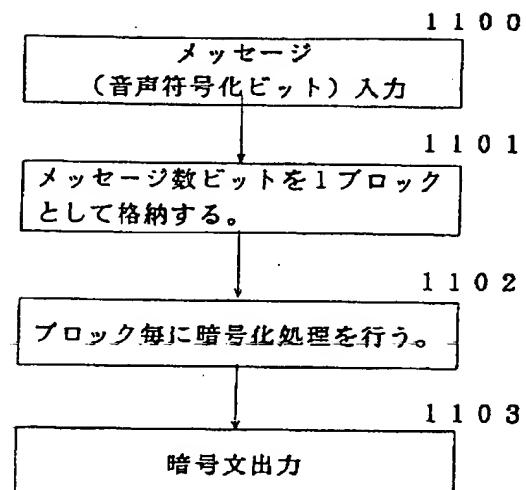
【図14】

図14



【図19】

図19



【図15】

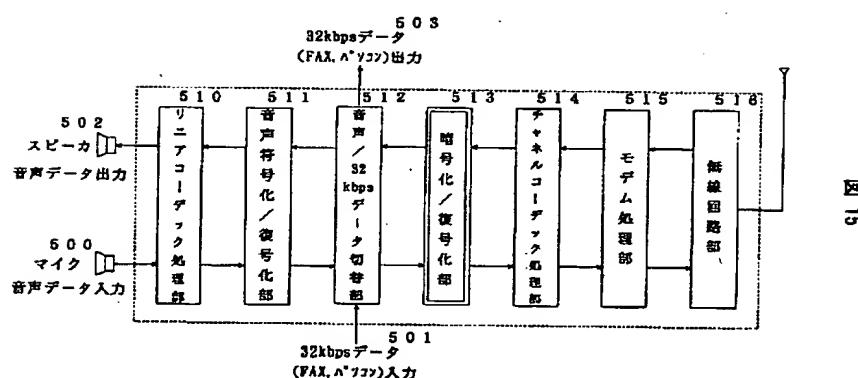
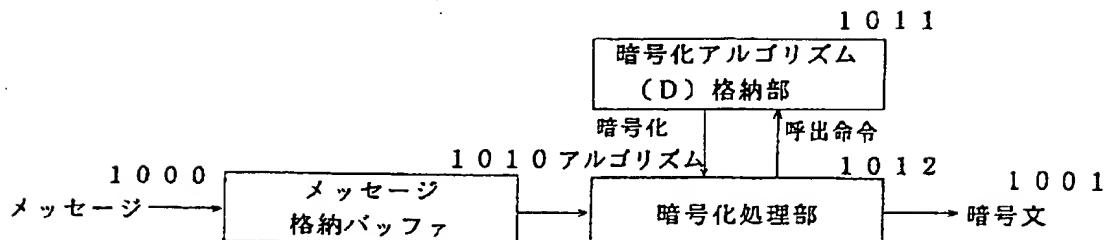


図15

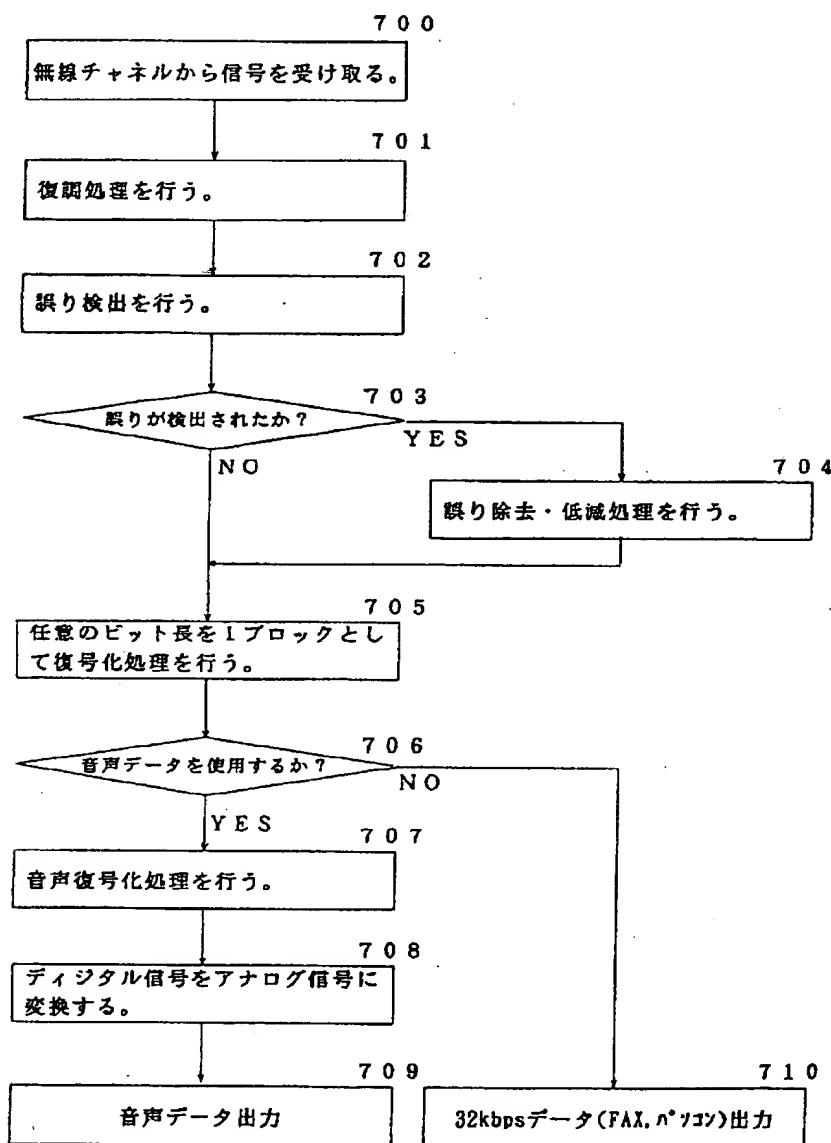
【図18】

図18



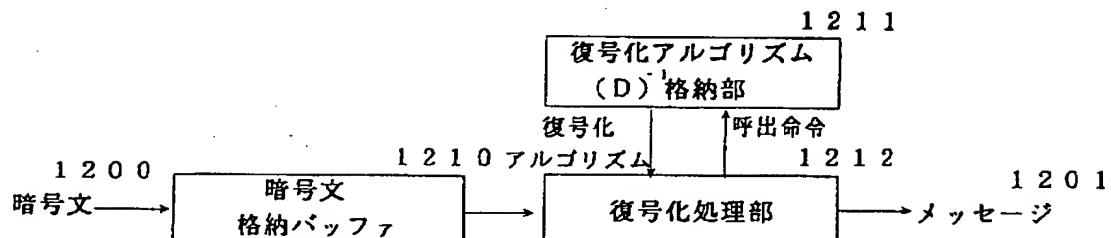
【図17】

図17



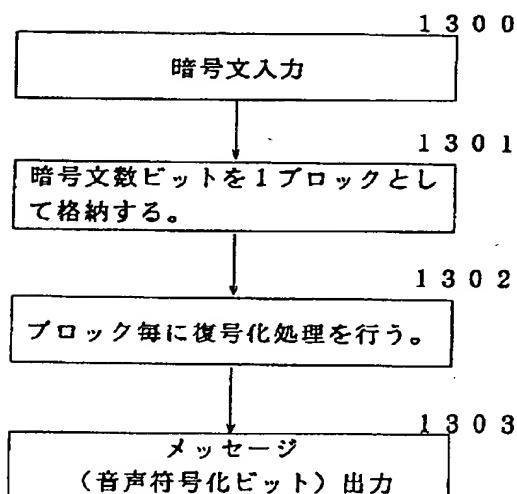
【図20】

図 20



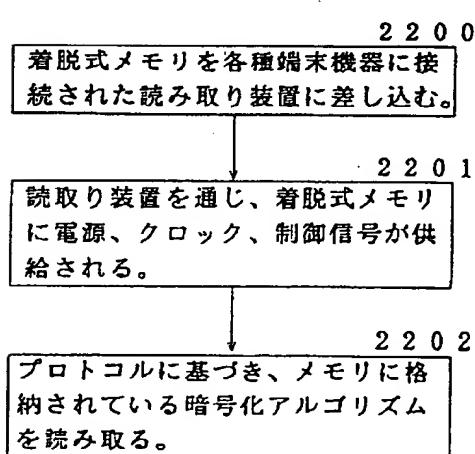
【図21】

図 21



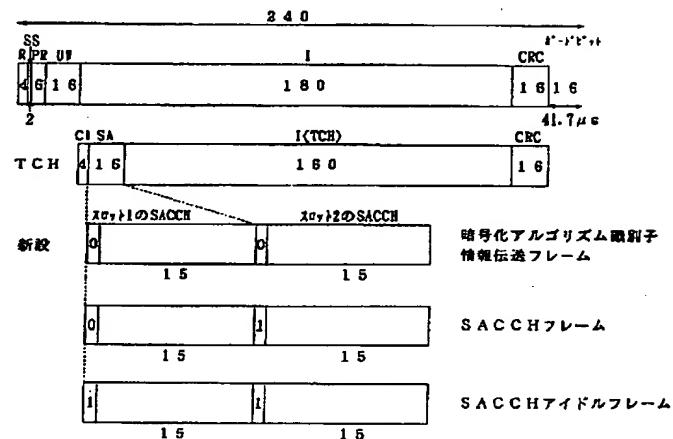
【図30】

図 30



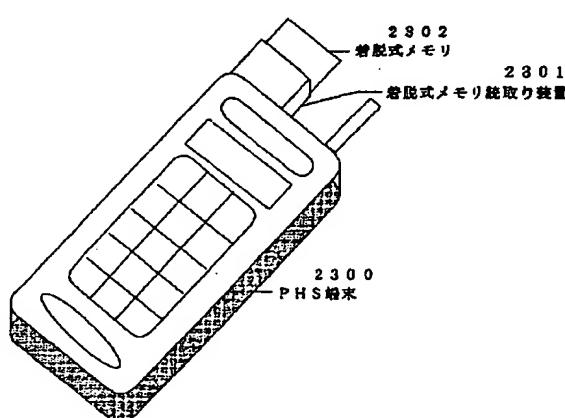
【図26】

図 26

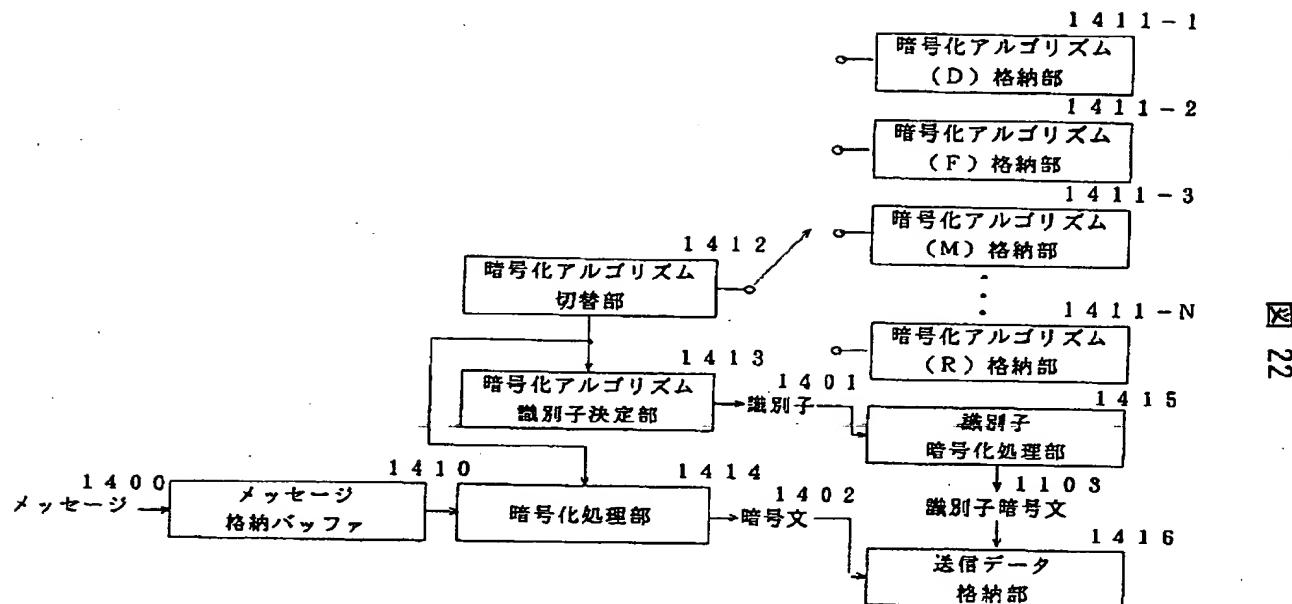


【図31】

図 31

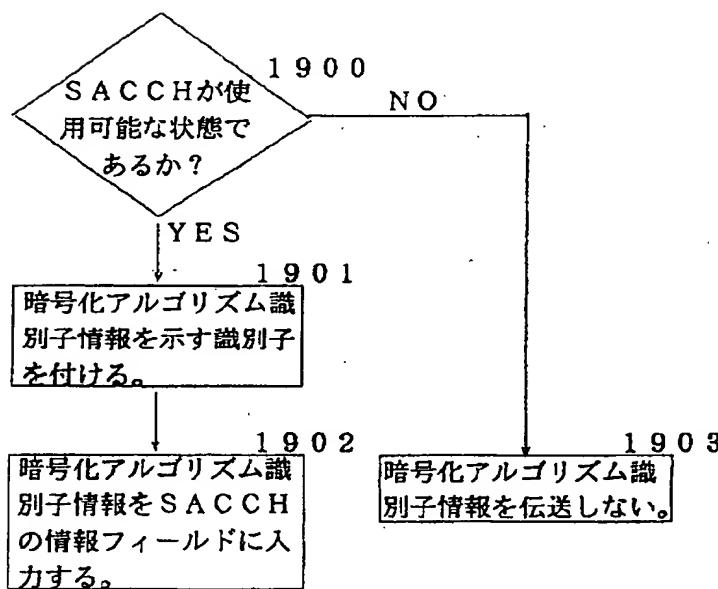


【図22】

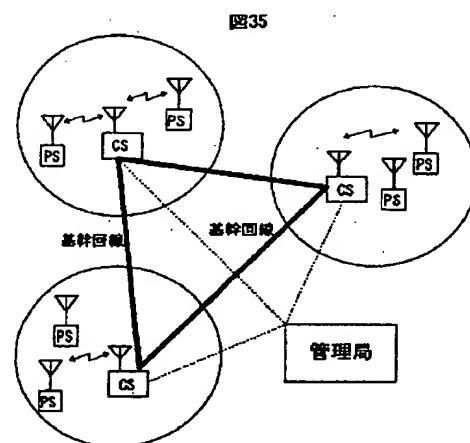
図
22

【図27】

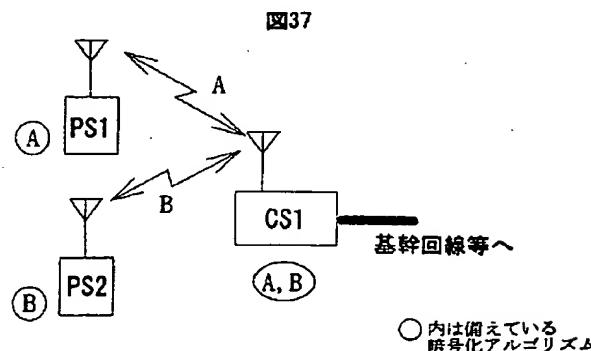
図 27



【図35】



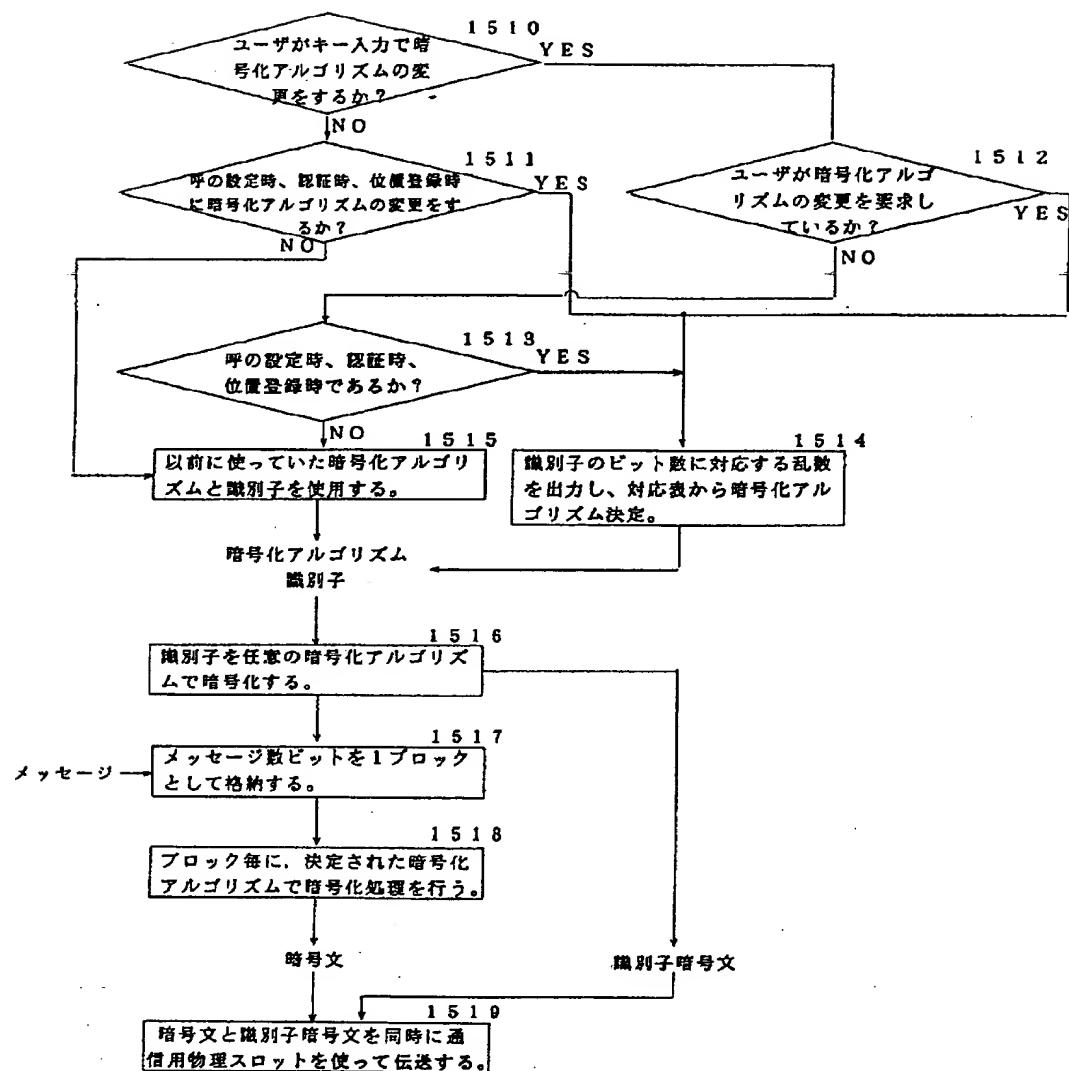
【図37】



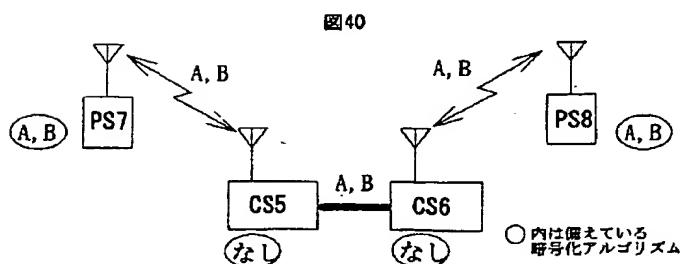
○ 内は備えている
暗号化アルゴリズム

【図23】

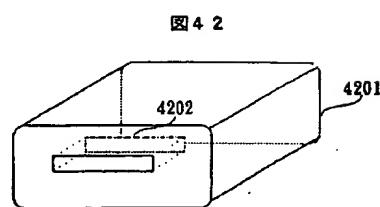
図 23



【図40】

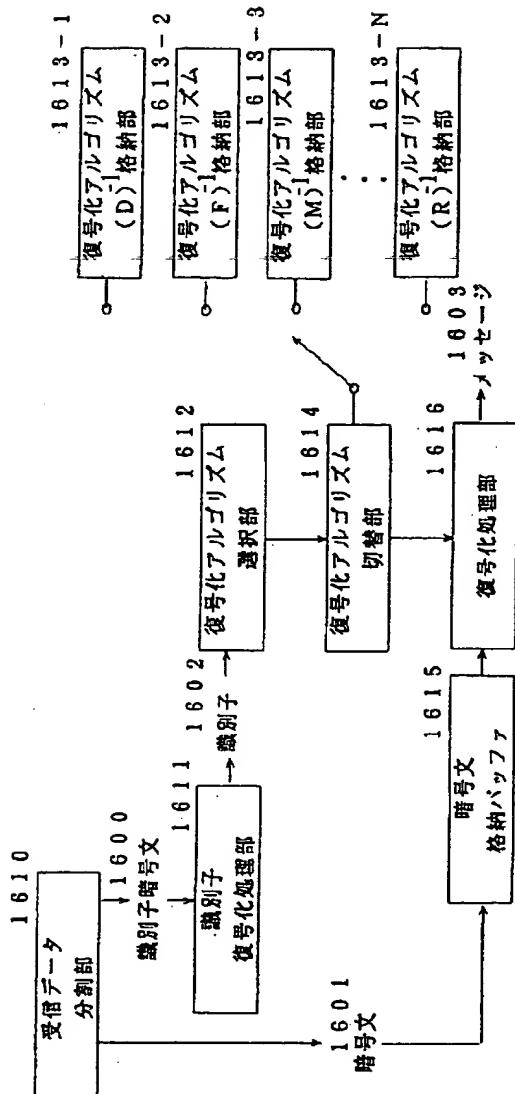


【図42】



[図24]

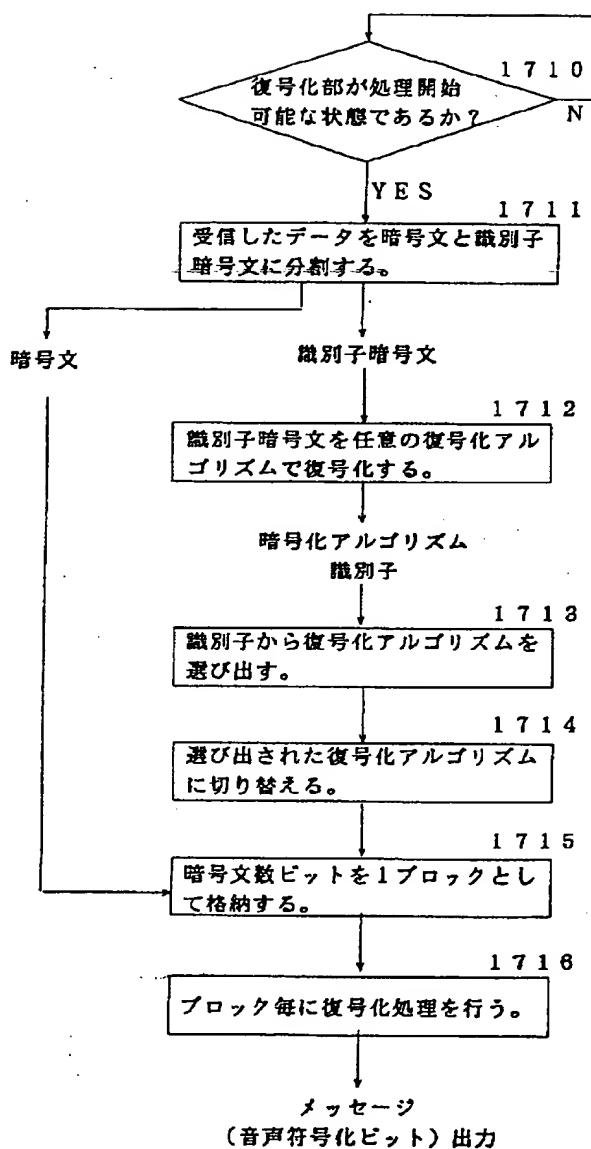
図 24



注) 図中の復号化アルゴリズム格納部の中の
-1は暗号化アルゴリズムの逆関数を示す。

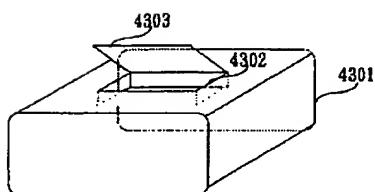
【図25】

図 25



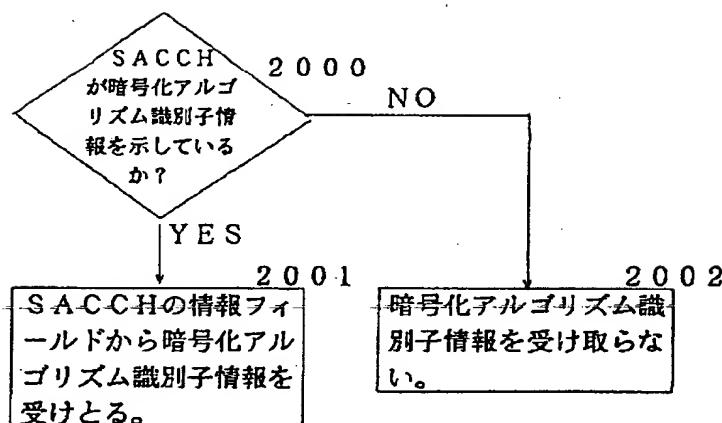
【図43】

図43

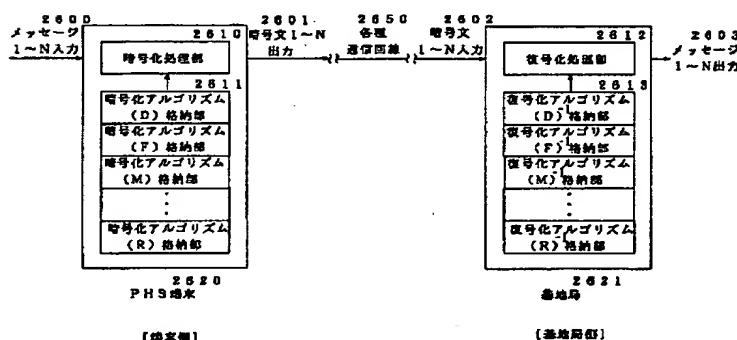


【図28】

図 28



【図34】

図
34

【図38】

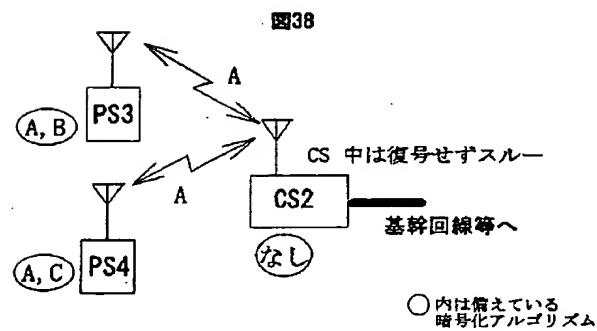


図38

【図39】

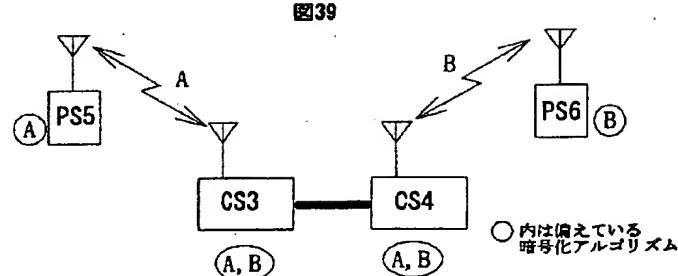
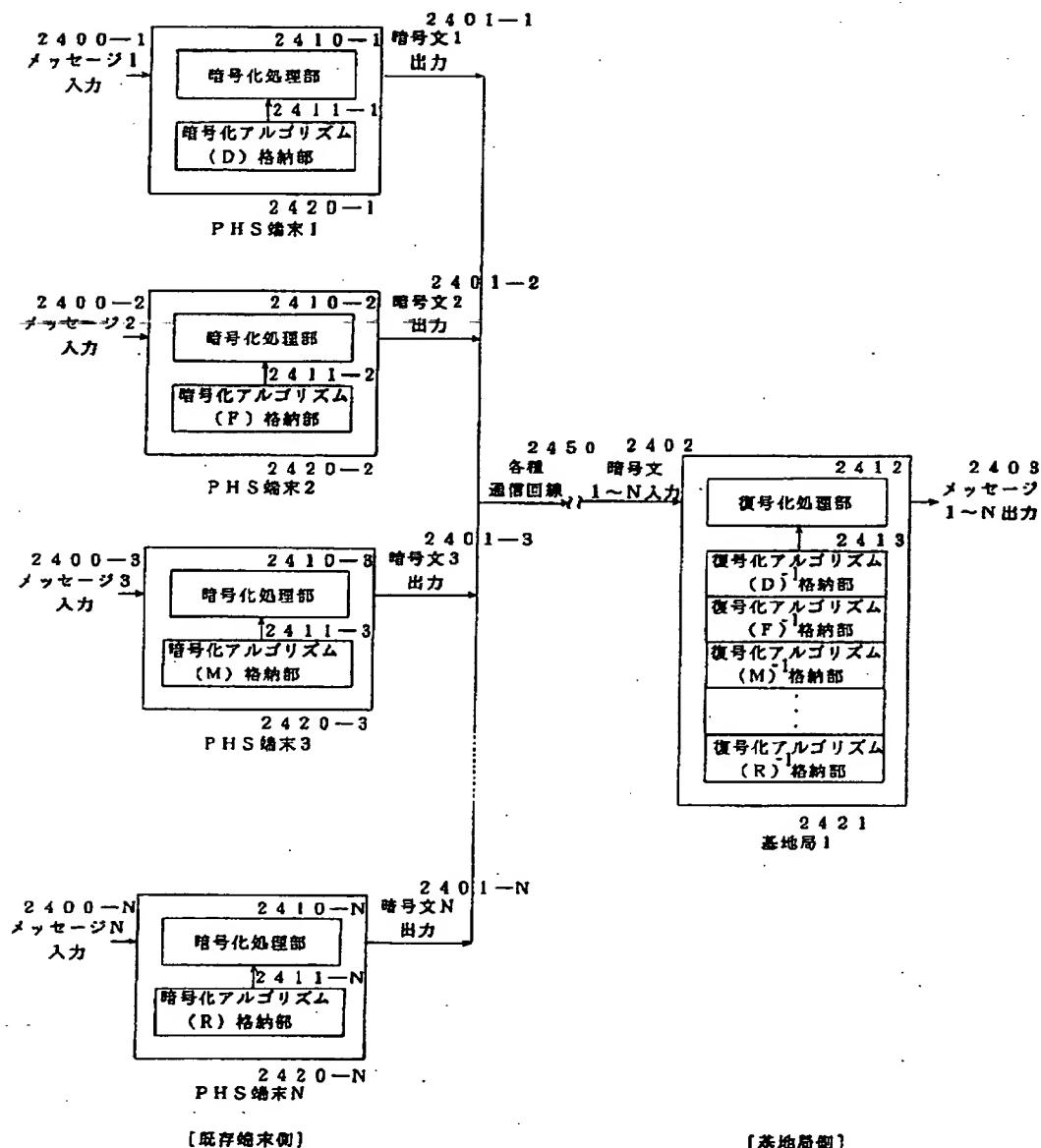


図39

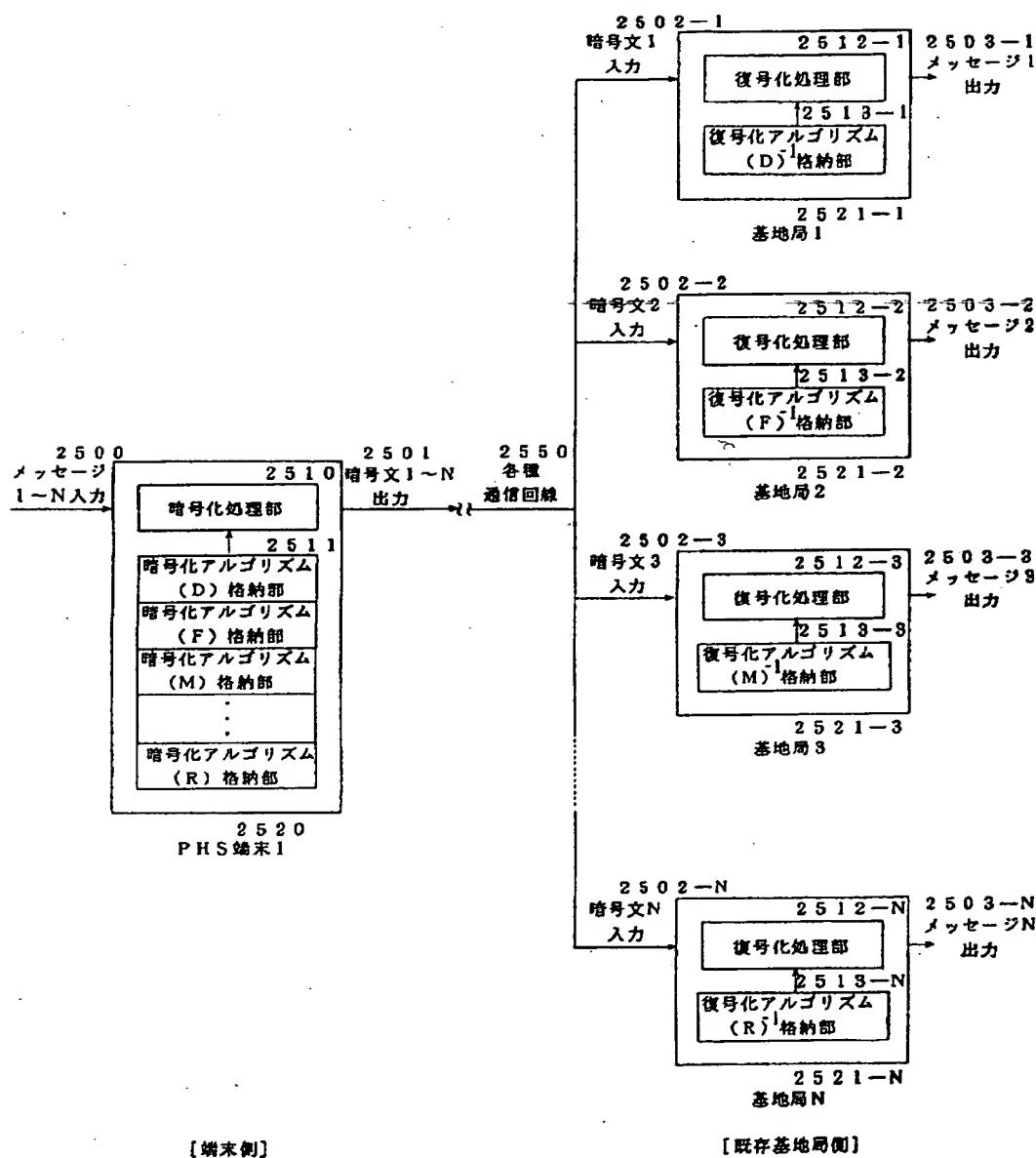
【図32】

図 32



【図33】

図 33



【端末側】

【既存基地局側】